ESTADO DA ARTE DA CRIPTOGRAFIA DE CHAVE PÚBLICA BASEADA NO "PROBLEMA DA MOCHILA"

Aldner Peres de Oliveira

TESE SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS (M.Sc.) EM ENGENHARIA DE SISTEMAS E COMPUTAÇÃO.

Aprovada por :

Prof. Antonio A. F. de Oliveira
(Presidente)

Prof. Almir Paz de Lima

Prof. Cláudio Bornstein

Prof. Jaime Szwarcfiter

RIO DE JANEIRO, RJ - BRASIL

ABRIL DE 1988

FICHA CATALOGRÁFICA

OLIVEIRA, ALDNER PERES DE

Estado da Arte da Criptografia de Chave Pública baseada no "Problema da Mochila" , [Rio de Janeiro] 1988.

XI , 300 p. , 29,7 cm (COPPE/UFRJ , M.Sc.,Engenharia de Sistemas e Computação, 1988)

Tese - Universidade Federal do Rio de Janeiro, COPPE.

1. Sistemas Criptográficos de Chave Pública baseados no Problema da Mochila . I. COPPE/UFRJ II. Título (série).

AGRADECIMENTOS

A Deus, que me conduziu durante a realização deste trabalho, meu eterno agradecimento...

Aos meus superiores e demais amigos do Centro de Análises de Sistemas Navais, agradeço a amizade, o incentivo e o imprescindível apoio moral e material que tanto contribuíram para a elaboração desta tese.

À minha família, agradeço os sacrifícios suportados ao longo destes anos, em que as horas consumidas em estudos não me permitiram dedicar a necessária atenção aos familiares.

Ao Prof. Antonio A. F. de Oliveira, agradeço a compreensão, o incentivo e a boa vontade sempre demonstrados nas ocasiões em que foi solicitado, sem o que, indubitavelmente, não teria sido possível a conclusão desta tese.

Ao Prof. Almir Paz de Lima, um agradecimento especial pela orientação segura e pelo apoio prestados nos momentos mais difíceis. Mais que orientador, um amigo e entusiasta das atividades de ensino, em particular da Criptografia. Aqui apresento meus sinceros agradecimentos pela atenção e incansável dedicação demonstradas, quando de minhas muitas consultas, no esclarecimento das dúvidas surgidas, e também pelas sugestões apresentadas no decorrer do desenvolvimento dos trabalhos, que me permitiram levar a bom termo esta tese.

Agradeço, ainda, a todos quantos, direta ou indiretamente, contribuíram para a finalização desta tese.

RESUMO

Resumo da Tese apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.).

ESTADO DA ARTE DA CRIPTOGRAFIA DE CHAVE PÚBLICA BASEADA NO "PROBLEMA DA MOCHILA"

Aldner Peres de Oliveira

Abril / 1988

Orientadores : Prof. Antonio A. F. de Oliveira
Prof. Almir Paz de Lima
Programa : Engenharia de Sistemas e Computação

Esta tese trata da criptografia de chave pública baseada no problema da mochila ("Knapsack Problem").

A formulação matemática, os conceitos e características básicas, assim como as vantagens e desvantagens do primeiro criptossistema mochila de chave pública - aquele idealizado por Merkle e Hellman em 1978 - são abordados inicialmente.

Apresentam-se, a seguir, estudo comparativo e análise crítica dos diversos trabalhos surgidos a partir de então: uns, como o de Shamir (1982), explorando vulnerabilidades e apontando métodos de ataques criptoanalíticos, outros propondo aprimoramentos técnicos visando a obter um sistema resistente a tais possibilidades de criptoanálises.

Nesse estudo, sem respeitar a ordem cronológica, os métodos de ataque são agrupados de acordo com a abordagem criptoanalítica, e as formulações de novos criptossistemas são classificadas segundo suas características e propriedades de construção, o que pode ser considerado uma contribuição para a literatura existente sobre o assunto.

Uma discussão abrangente sobre o emprego e aspectos de segurança de criptossistemas de chave pública baseados no "problema da mochila" conclui o presente estudo.

ABSTRACT

Abstract of Thesis presented to COPPE/UFRJ as partial fulfillment of the requirements for the degree of Master of Science (M.Sc.).

STATE OF THE ART OF THE PUBLIC KEY CRYPTOGRAPHY BASED ON THE KNAPSACK PROBLEM

Aldner Peres de Oliveira

April / 1988

Chairman : Prof. Antonio A. F. de Oliveira
Advisor : Prof. Almir Paz de Lima
Department : Engenharia de Sistemas e Computação

This thesis deals with the public key cryptography based on the Knapsack Problem.

The mathematical formulation, the concepts and the basic characteristics as well as the advantages and disadvantages of the first knapsack public key cryptosystem - that was idealized by Merkle and Hellman in 1978 - are dealt formerly.

A comparative study and a critical analysis of various works produced since then are presented. Some, as that of Shamir (1982), exploring vulnerabilities and pointing at cryptoanalytic attacking methods, others suggesting technical improvements aiming at obtaining a system resistent to such possibilities of cryptoanalysis.

In this study, without respect to chronological order, the attacking methods are grouped in accordance to the breaking approach, and the new cryptosystems formulations are classified on their characteristics and construction properties, what may be considered a contribution to the existing literature on the subject.

A broad discussion regarding the employment and security aspects of public key cryptosystems based on the knapsack problem concludes the present thesis.

ÍNDICE

CAPÍTULO I

INTRODUÇÃO

I.1 - MOTIVAÇÃO E OBJETIVO DA PESQUISA

O importante papel desempenhado pela criptografia nos meios militares despertou o meu interesse pelo seu estudo e motivou a elaboração desta tese.

Com intuito de aumentar meus conhecimentos na área de criptologia e, desta forma, tentar trazer alguma contribuição para as aplicações diárias no meu ambiente de trabalho, escolhi, dentre os vários métodos criptográficos existentes, estudar mais detalhadamente os sistemas criptográficos de chave pública tipo mochila, pois estes sistemas apresentam características peculiares que ficarão evidentes ao longo deste trabalho.

A presente tese tem como propósito apresentar vários criptossistemas de chave pública baseados no algoritmo da mochila; mais especificamente determinar, aproximadamente, o estado da arte do problema da mochila em aplicações criptográficas.

Para consecução deste propósito, a tese foi elaborada de forma a conter as seguintes partes :

No capítulo I são apresentadas as razões que motivaram a pesquisa, e também o propósito final deste estudo. É apresentada, ainda, uma descrição breve sobre a criptografia de chave pública: seus conceitos e características básicas e os motivos que geraram o aparecimento dos criptossistemas de chave pública. A finalidade é facilitar a compreensão dos demais capítulos.

No capítulo II é realizado um estudo do algoritmo da mochila, mostrando a sua utilização na criptofrafia de chave pública. Primeiramente é apresentada uma descrição detalhada do problema da mochila, com a definição formal de mochila supercrescente e mochila "trapdoor", apresentando, para o primeiro caso, um algoritmo para solução do problema mochila associado, com um exemplo de aplicação. Finalmente a mochila é apresentada como um

sistema criptográfico de chave pública. É descrita a formulação matemática do sistema criptográfico de chave pública tipo mochila proposto por Merkle e Hellman (SCMH), com seus conceitos básicos, definições e características. São apresentados os métodos básico (iteração simples) e iterativo (iteração múltipla), sendo evidenciadas as diferenças entre eles e apresentado um exemplo numérico para ilustrar cada caso. Ao final do capítulo são listadas as vantagens e desvantagens da utilização do SCMH.

No capítulo III são mostradas algumas propostas de ataques criptoanalíticos aos sistemas de chave pública tipo mochila, selecionadas da literatura. É realizada uma análise crítica da adequabilidade de cada método, sendo ressaltados os aspectos que podem tornar viáveis esses ataques.

No capítulo IV são apresentadas algumas outras formulações, disponíveis na literatura, para criptossistemas de chave pública baseados no algoritmo da mochila, sugeridas por vários autores com intuito de tentar desenvolver um sistema criptográfico resistente aos ataques criptográficos. Com isso pretende-se identificar um sistema que seja mais seguro, do ponto de vista criptoanalítico, que o sistema de Merkle-Hellman. Para cada formulação é apresentada a conceituação básica e são feitos comentários sobre sua segurança criptográfica.

No capítulo V são apresentadas as conclusões decorrentes da pesquisa, baseadas e fundamentadas nos capítulos anteriores. Ainda com base no estudo realizado sobre o criptossistema de chave pública baseado no algoritmo da mochila, são feitas sugestões e recomendações quanto à sua utilização nos diversos casos, ressaltando-se também as restrições de seu emprego, quando existirem. São ainda indicadas as sugestões para teses futuras, com a enumeração daquelas questões que surgiram durante o trabalho, e para as quais não tenham sido encontradas respostas ou que requeiram estudos e pesquisas além do limite deste trabalho.

Com esta tese pretende-se analisar vários algoritmos tipo mochila, existentes na literatura, que sejam aplicáveis a sistemas criptográficos, verificando a eficiência e possíveis pontos fracos de cada um.

I.2 - NOÇÕES SOBRE CRIPTOGRAFIA DE CHAVE PÚBLICA

Com a finalidade de facilitar a compreensão dos capítulos subseqüentes são apresentadas, a seguir, noções gerais sobre criptografia e são mostrados os conceitos e características básicas dos sistemas criptográficos de chave pública. Para maiores detalhes sobre o assunto é recomendada a leitura das referências [5],[7],[8],[18],[20],[22],[23],[24],[63] e [64].

A criptografia é o ramo da criptologia - arte e ciência da comunicação secreta - que compreende os métodos e processos de transformação de uma "mensagem" escrita na forma corrente (texto claro), a uma forma ininteligível (criptograma) para um elemento que não tem acesso autorizado à mensagem. A reconversão do texto cifrado, ou criptograma, para a mensagem original é feita usando-se o inverso do processo de transformação.

O processo pelo qual o texto claro (forma inteligível) é transformado em criptograma (forma ininteligível) é chamado de cifração, e aquele pelo qual o criptograma é transformado em texto claro é chamado de decifração. A parte essencial destes processos - o segredo compartilhado pelos usuários autorizados - é referenciada como a "chave", informação da qual dependem os processos de cifração e de decifração.

O mecanismo que processa a transformação do texto claro para o criptograma e vice-versa, seja um conjunto de instruções, um programa, ou uma parte de um equipamento eletrônico, é chamado de sistema criptográfico, criptossistema ou simplesmente sistema.

Quando um conjunto de dados valiosos ou secretos deve ser armazenado ou transmitido, esse conjunto é frequentemente protegido por técnicas de criptografia, usando transformações de dados a fim de torná-los inúteis ao inimigo. Tais transformações provêem solução para dois grandes problemas de segurança de dados : o problema de "privança", impedindo ao inimigo a extração de informação de um canal de comunicação, e o problema de "autenticação", impedindo ao inimigo a injeção de dados falsos no canal de transmissão ou a alteração de mensagens.

Há ainda o problema da "assinatura digital" de mensagens. A assinatura digital assegura ao receptor de uma mensagem a legitimidade de seu emissor, isto é, a assinatura identifica o emissor da mensagem. A essência da assinatura digital é que, apesar de somente uma pessoa poder produzí-la, qualquer pessoa pode reconhecê-la.

Um sistema criptográfico ideal deveria permitir a construção de criptogramas teoricamente indecifráveis. Porém, face às dificuldades de natureza prática, uma solução de compromisso consiste em usar métodos imperfeitos do ponto de vista teórico mas que tenham condições de resistir, por tempo suficiente, à análise do inimigo.

A criptoanálise (análise e quebra de cifra) é o processo pelo qual o inimigo tenta recuperar o texto claro, sem o conhecimento da chave de decifrar.

De acordo com a conceituação criptográfica tradicional, para haver comunicação segura em canais inseguros, é necessário transmitir a chave, usando um meio seguro (chamado "canal da chave") antes das mensagens cifradas poderem ser transmitidas seguramente. A razão pela qual não se utiliza o "canal da chave" para comunicações normais é que este é caro e inconveniente por ser demorado.

A dificuldade de distribuição de chaves tem sido uma das maiores limitações ao uso da tecnologia criptográfica convencional. Para que o emissor e o receptor de uma mensagem possam fazer uso de um canal fisicamente seguro para distribuição de chaves, eles devem estar preparados para esperar enquanto as chaves estão sendo enviadas, ou então têm que fazer uma preparação prévia para a comunicação criptográfica.

Em aplicações militares a Cadeia de Comando ajuda a limitar o número de conexões entre os usuários, mas, assim mesmo, o problema de distribuição de chaves tem sido um grande empecilho ao emprego da criptografia. Este problema é mais acentuado em aplicações de comunicação comercial em larga escala (como transferência eletrônica de fundos e correio computadorizado), onde o número de conexões cresce na ordem $(n^2-n)/2$, sendo n o número de usuários. Por isso, devido ao problema de distribuição de chaves, muitas vezes o custo de sistemas criptográficos convencionais torna-se proibitivo.

Uma solução elegante para simplificar o problema de distribuição de chaves é conseguida com o uso de "sistemas de chave pública".

O conceito fundamental, no qual os criptossistemas de chave pública se baseiam, é a observação simples e óbvia de que não há necessidade do processo e da chave de cifrar serem respectivamente iguais ao processo e à chave de decifrar.

Um criptossistema de chave pública pode ser definido como o sistema no qual as conversões de texto claro para criptograma e de criptotrama para texto claro são feitas utilizando-se diferentes chaves. Além disso, dada uma das chaves é quase tão difícil descobrir a outra como seria descobrir o texto claro dada somente uma amostra do criptograma. Esta separação das chaves para cifrar e decifrar torna possível liberar uma (a chave pública) enquanto a outra (a chave secreta) é mantida em segredo. Num sistema de chave pública, um canal de comunicação seguro, ou outro meio seguro, não é, em princípio, necessário para transmitir chaves, pois a mensagem pode ser cifrada usando-se a chave de cifrar do destinatário pretendido, que é revelada publicamente. Em princípio, somente ele pode decifrar a mensagem, pois somente ele conhece a correspondente chave de decifrar.

Como é computacionalmente inviável obter a chave de decifrar a partir da chave de cifrar, esta última pode ser fornecida publicamente sem comprometer a outra. Desta forma, cada usuário do sistema de chave pública pode colocar sua chave de cifrar numa lista pública, mantendo em segredo a sua correspondente chave de decifrar. Isso possibilita a um usuário do sistema cifrar uma mensagem de modo que somente o destinatário pretendido seja capaz de decifrá-la. Cada usuário envia mensagens, para um outro, cifradas com a chave pública de cifrar do receptor, e decifra as mensagens que recebe usando sua própria chave secreta de decifrar (e neste caso não há necessidade de saber a identidade de quem enviou a mensagem).

Para construção dessas chaves são utilizadas, em alguns sistemas criptográficos, as chamadas funções "trapdoor one-way", isto é, funções alçapão de "mão-única". Essas funções são chamadas de "mão-única" porque são facilmente computadas em uma direção, porém são muito difíceis de serem computadas na

outra direção. Elas são chamadas de "alçapão" pois as funções inversas são, de fato, facilmente computadas desde que seja conhecida uma certa informação "alçapão".

Os conceitos sobre criptografia de chave pública foram introduzidos por DIFFIE e HELLMAN [1], no seu trabalho pioneiro publicado em meados de 1976, no qual mostraram ser possível desenvolver sistemas criptográficos de chave pública, e apresentaram suas aplicações potenciais, sem, no entanto, descreverem implementações práticas.

Em fins de 1977 RIVEST, SHAMIR e ADLEMAN [2] desenvolveram o primeiro criptossistema de chave pública, chamado sistema RSA (iniciais de seus autores), elaborado a partir da Teoria dos Números. Este sistema se baseia nos conceitos de números primos e na relativa facilidade com que um par de primos pode ser multiplicado, comparada com a dificuldade de fatorar o seu produto para descobrir esses primos.

No início de 1978, MERKLE e HELLMAN [3] apresentaram um segundo criptossistema de chave pública, chamado de Sistema "Trapdoor Knapsack" (mochila alçapão), usado para cifrar e decifrar mensagens; as raízes deste sistema estão no campo conhecido como Matemática Combinatória. Este sistema é baseado no algoritmo da mochila e nos conceitos de função "trapdoor one-way" (função alçapão de mão-única). Utiliza uma seqüência supercrescente como chave secreta de decifrar, a partir da qual é obtida a chave pública de cifrar empregando-se multiplicações modulares, sendo o multiplicador e o módulo (informação "trapdoor") mantidos secretos. Merkle e Hellman propuseram dois métodos: o método básico (de iteração simples), e o método iterativo (de iteração múltipla), tendo sido este último introduzido " para aumentar a segurança do método básico ".

A partir do aparecimento do sistema criptográfico de Merkle-Hellman (SCMH), começaram a surgir vários trabalhos sobre os criptossistemas de chave pública tipo mochila. Alguns trabalhos apresentando métodos de ataque criptoanalítico ao SCMH e a outros criptossistemas similares. Outros trabalhos apresentando novas formulações para os criptossistemas de chave pública, de modo a tentar superar esses ataques.

O estudo e a análise crítica desses vários trabalhos é o objeto da presente tese.

CAPÍTULO II

UTILIZAÇÃO DO "PROBLEMA DA MOCHILA" PARA FINS CRIPTOGRÁFICOS

II.1 - CONSIDERAÇÕES SOBRE O "PROBLEMA DA MOCHILA"

II.1.1 - DEFINIÇÃO DO "PROBLEMA DA MOCHILA"

O problema da mochila, também conhecido como problema da soma de subconjuntos, é um problema de combinatória, e apresenta a seguinte formulação básica :

"Dada uma mochila de tamanho S e um conjunto de n cilindros, todos de mesmo diâmetro da mochila e alturas a_1, a_2, a_3,...,a_n , encontrar um subconjunto de cilindros que encha completamente a mochila."

A formulação matemática formal para o problema da mochila é :

"Dados um conjunto de inteiros $a = \{ a_1, a_2, \ldots, a_n \}$ e um inteiro S , determinar, se existir, um subconjunto de $\{ a_i \}_{i=1,n}$ tal que a soma de seus elementos seja igual a S. Equivalentemente, dados o vetor $a = (a_1, a_2, \ldots, a_n)$ e um inteiro S , encontrar um vetor binário $x = (x_1, x_2, \ldots, x_n)$ de n elementos, se existir, tal que $S = a.x^T$.

Para o problema geral da mochila os coeficientes do vetor $x = (x_1, x_2, \ldots, x_n)$ são inteiros positivos, em vez de dígitos binários 0 ou 1.

O problema da mochila pertence à classe NP-completa [63].

Uma função é dita pertencer à classe de complexidade "P" (polinomial) se ela puder ser computada por uma máquina determinística de Turing num tempo limitado superiormente por alguma função polinomial do tamanho de sua entrada. Pode-se considerar esta classe como aquela em que as funções são computadas facilmente, porém é mais preciso dizer que uma função que não pertence a esta classe deve ser mais difícil de computar para, pelo menos, algumas entradas.

Uma função pertence à classe "NP" (não polinomial) se não for calculável deterministicamente em tempo polinomial por alguma técnica conhecida.

Existe ainda uma subclasse de funções "NP", conhecida como classe NP-completa, com as seguintes propriedades interessantes [65] :

- o tempo para o cálculo da solução de uma função NP-completa cresce exponencialmente com o tamanho do problema, mesmo utilizando-se os melhores algoritmos conhecidos;
- uma vez determinada uma solução para uma função NP-completa, ela pode ser testada num tempo extremamente pequeno (linear);
- nenhum problema NP-completo pode ser resolvido por algum algoritmo polinomial conhecido; e
- Se existir um algoritmo polinomial para algum problema NP-completo, então existirão algoritmos polinomiais para todos os problemas NP-completos.

O significado prático do conceito de problema NP-completo repousa na crença de que tais problemas são intratáveis do ponto de vista computacional; que eles não são susceptíveis a soluções algorítmicas eficientes; e que qualquer algoritmo que resolva corretamente um problema NP-completo exigirá, no pior caso, tempo exponencial e,desta forma, será impraticável, exceto para os casos em que o problema for muito pequeno.

Para uma mochila de tamanho n, onde n é o número de elementos do vetor mochila, são necessárias 2^n tentativas para determinar a solução pelo método de exaustão e, portanto, para valores grandes de n, por exemplo $n \geq 100$, torna-se quase impossível determinar a solução por este processo.

A afirmativa de que o problema mochila é NP-completo significa que existe pelo menos um problema mochila difícil de ser resolvido. No entanto, existem mochilas para as quais a solução do problema mochila associado pode ser facilmente determinada. Se não for feita nenhuma restrição quanto aos valores dos elementos do vetor $a = (a_1, a_2, \ldots, a_n)$ (por exemplo os elementos formarem uma seqüência supercrescente), não necessariamente existirá solução para o problema mochila associado, ou, então, poderão existir várias soluções.

II.1.2 - MOCHILA SUPERCRESCENTE

Se o vetor mochila $a = (a_1, a_2, \ldots, a_n)$ for escolhido de modo que cada elemento seja maior que a soma dos elementos precedentes, isto é, os elementos formam uma seqüência supercrescente definida por:

$$a_i > \sum_{j=1}^{i-1} a_j \quad , \quad i \geq 2$$

e cada x_i for 0 ou 1, então o problema da mochila torna-se muito simples, e neste caso o vetor solução $x = (x_1, x_2, \ldots, x_n)$ pode ser determinado, ou mostrado não existir, com,no máximo, n subtrações, conforme o algoritmo apresentado mais adiante.

O fato de a seqüência $a = (a_1, a_2, \ldots, a_n)$ ser supercrescente implica que:

- a representação de $S \left(= \sum_{i=1}^{n} a_i . x_i \right)$, quando possível, é única, pois devido à lei de formação dos elementos da mochila supercrescente, os 2^n subconjuntos possíveis desta mochila apresentam valores distintos para a soma de seus elementos ; e

- esta representação pode ser encontrada com, no máximo, n passos computacionais.

A seguir são apresentados o algoritmo para solução de mochila supercrescente e um exemplo numérico de resolução deste tipo de mochila.

II.1.2.1 - ALGORITMO PARA SOLUÇÃO DE MOCHILA SUPERCRESCENTE

Seja o seguinte problema mochila supercrescente :

$$a = (a_1, a_2, \ldots, a_n)$$

$$a_i > \sum_{j=1}^{i-1} a_j \quad , \quad i \geq 2$$

$$a_1 > 0 \quad \text{e} \quad a_i \text{ inteiro para } i = 1, \ldots, n$$

$$x = (x_1, x_2, \ldots, x_n) \quad , \quad x_i = 0 \text{ ou } 1$$

$$S = \sum_{i=1}^{n} a_i . x_i$$

Para determinar os elementos do conjunto $\{ a_i \}_{i=1,n}$ cuja soma fornece o valor S , utiliza-se o algoritmo :

INÍCIO

FAÇA $k := n$ e $S_k := S$

ENQUANTO $k > 0$ FAÇA :

SE $S_k \geq a_k$ ENTÃO:

$x_k := 1$ (a_k é elemento do subconjunto)

$S_{k-1} := S_k - a_k$

SE $S_k < a_k$ ENTÃO :

$x_k := 0$ (a_k não é elemento do subconjunto)

$S_{k-1} := S_k$

FAÇA $k := k - 1$

SE $S_0 = 0$ ENTÃO :

$(x_i)_{i=1,n}$ é a solução procurada

SENÃO Não existe solução para o problema.

FIM

II.1.2.2 - EXEMPLO DE RESOLUÇÃO DE SEQÜÊNCIA SUPERCRESCENTE

Seja a seqüência supercrescente :

a = (3,5,11,20,41,83,169,340,679,1358)

e seja S = 1260.

Determinar o subconjunto de $\{a_i\}_{i=1,10}$ cuja soma é igual a S.

SOLUÇÃO :

$$S = a_1x_1 + a_2x_2 + \ldots + a_9x_9 + a_{10}x_{10} \quad , \quad x_i = 0 \text{ ou } 1$$

$$1260 = 3x_1 + 5x_2 + 11x_3 + 20x_4 + 41x_5 + 83x_6 + 169x_7 + 340x_8 + 679x_9 + 1358x_{10}$$

Para determinar o vetor $(x_i)_{i=1,10}$ basta aplicar o algoritmo apresentado no item II.1.2.1 :

$k = n = 10$ $\qquad S_{10} = S = 1260$

$1260 < 1358 \rightarrow x_{10} = 0$

$k = 9$ $\qquad S_9 = 1260$

$1260 > 679 \rightarrow x_9 = 1$

$k = 8$ $\qquad S_8 = 1260 - 679 = 581$

$581 > 340 \rightarrow x_8 = 1$

$k = 7$ $\qquad S_7 = 581 - 340 = 241$

$241 > 169 \rightarrow x_7 = 1$

$k = 6$ $\qquad S_6 = 241 - 169 = 72$

$72 < 83 \rightarrow x_6 = 0$

$k = 5$ $\qquad\qquad$ $S_5 = 72$

$72 > 41 \quad \rightarrow \quad x_5 = 1$

$k = 4$ $\qquad\qquad$ $S_4 = 72 - 41 = 31$

$31 > 20 \quad \rightarrow \quad x_4 = 1$

$k = 3$ $\qquad\qquad$ $S_3 = 31 - 20 = 11$

$11 = 11 \quad \rightarrow \quad x_3 = 1$

$k = 2$ $\qquad\qquad$ $S_2 = 11 - 11 = 0$

$0 < 5 \quad \rightarrow \quad x_2 = 0$

$k = 1$ $\qquad\qquad$ $S_1 = 0$

$0 < 3 \quad \rightarrow \quad x_1 = 0$

$k = 0$ $\qquad\qquad$ $S_0 = 0$

O vetor solução é :

$x = (0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$

o que corresponde ao seguinte subconjunto de $\{ a_i \}_{i=1,10}$:

$\{ 11, 20, 41, 169, 340, 679 \}$

pois :

$11 + 20 + 41 + 169 + 340 + 679 = 1260 = S$

II.1.3 - MOCHILA "TRAPDOOR"

Um problema mochila supercrescente fácil pode ser convertido em um problema mochila difícil escolhendo-se um par de números inteiros aleatórios w e M (chamado par "trapdoor") tal que (w,M) = 1, isto é, w e M são primos entre si, e $M > \sum_{i=1}^{n} a_i$.

Calcula-se, então, o vetor difícil $b = (b_1,\ldots,b_n)$ da seguinte forma :

$$b_i = w \cdot a_i \mod M \quad , \quad 1 \leq i \leq n$$

onde : $0 \leq b_i < M$ para $i = 1,\ldots,n$;

$a = (a_1,a_2,\ldots,a_n)$ é o vetor fácil ;

$b = (b_1,b_2,\ldots,b_n)$ é o vetor "trapdoor" difícil.

Em geral espera-se ser difícil resolver o problema da mochila com $b = (b_i)_{i=1,n}$ em vez de $a = (a_i)_{i=1,n}$, se M e w forem desconhecidos. Se eles forem conhecidos, pode-se calcular, segundo [21], [45], [60], [61] ou [62], um inteiro $w^{-1} \mod M$ tal que :

$$w^{-1} \cdot w \equiv 1 \mod M$$

Para determinar $x = (x_i)_{i=1,n}$ tal que $S_b = b \cdot x^T$, para algum S_b , basta notar que :

$$S_b \cdot w^{-1} \equiv w^{-1} \cdot b \cdot x^T \mod M$$

ou

$$S_a \equiv a \cdot x^T \mod M$$

onde : $S_a \equiv w^{-1} \cdot S_b \mod M$ e $0 \leq S_a < M$

Com o valor S_a calculado, pode-se determinar, facilmente, o vetor $x = (x_i)_{i=1,n}$, pois o vetor $a = (a_i)_{i=1,n}$ é supercrescente.

II.2 - SISTEMA CRIPTOGRÁFICO DE MERKLE-HELLMAN (SCMH)

II.2.1 - CONSIDERAÇÕES INICIAIS

Dois exemplos clássicos de problema NP-completo são : problema do caixeiro viajante [65] e problema da mochila [63], entre outros.

Uma função f é dita ser uma função "one-way" (de mão-única ou unidirecional) de x se, para qualquer argumento x no domínio de f , é fácil computar o correspondente valor y = f(x), mas, para quase todo valor y no intervalo de f , é computacionalmente inviável resolver a equação $x = f^{-1}(y)$ para qualquer argumento x possível, utilizando-se um método prático.

Seguem-se as definições :

Definição II-1 : Uma função f é "fácil de resolver" se existe um algoritmo que resolve f em "P". A função f é "difícil de resolver" se nenhum algoritmo que resolve f pertence a "P". (Resolver uma função significa determinar o seu valor para qualquer argumento.)

Se for feita a hipótese de que f é uma representação injetiva ("one-to-one") do seu domínio X para sua imagem Y ,

$$f : X \rightarrow Y$$

então f^{-1} existe,

$$f^{-1} : Y \rightarrow X$$

Definição II-2 : Uma função f é uma função "one-way" se f é fácil de resolver, mas f^{-1} ou é difícil de resolver ou não existe.

Definição II-3 : Uma função f é uma função "trapdoor" (função alçapão) se :

(1) f é fácil de resolver e,

(2) existe alguma informação adicional ("passagem secreta") sem a qual f é uma função "one-way"; dada esta informação, f^{-1} existe e é fácil de resolver.

Parece ser possível construir um conjunto de funções "one-way" $f(n,x)$, no qual a dificuldade de computar o valor $y = f(n,x)$ cresce linearmente com n , mas a dificuldade de calcular $x = f^{-1}(n,y)$ cresce exponencialmente com n . Tal fato torna possível aumentar n até um certo valor para o qual o cômputo da função inversa atinge limites astronômicos em termos de dificuldade computacional.

Polinômios são um exemplo elementar de funções "one-way". É muito mais difícil, em geral, encontrar uma raiz x_0 da equação polinomial $p(x) = y$ do que calcular o polinômio $p(x)$ para $x = x_0$.

O criptossistema de chave pública proposto por MERKLE e HELLMAN [3] é baseado no problema da mochila (ou problema da soma de subconjuntos). Como já mencionado, este problema é considerado, em geral, difícil, pertencendo à classe de problemas NP-completos. No entanto, alguns problemas da mochila são muito simples, e a técnica de Merkle e Hellman sugere começar com um problema simples e convertê-lo para uma forma mais complexa. Eles observaram que, se uma mochila for construída adequadamente, certos detalhes dessa construção podem ser utilizados como uma chave secreta e, então, esta chave pode ser empregada em um sistema criptográfico. Esta mochila é denominada "trapdoor knapsack" (mochila alçapão).

II.2.2 - MÉTODO DE ITERAÇÃO SIMPLES

O método de iteração simples do sistema criptográfico de chave pública tipo mochila de Merkle-Helman é também conhecido como o método básico, pois corresponde à primeira formulação deste criptossistema.

O método básico consiste, genericamente, de um vetor de cifração (chave pública) $a = (a_1, a_2, \ldots, a_n)$, de um vetor de coeficientes binários (mensagem) $x = (x_1, x_2, \ldots, x_n)$, de parâmetros secretos w e M , e de um criptograma (texto cifrado) $S = \sum_{i=1}^{n} a_i . x_i$ que é enviado ao receptor autorizado.

Os processos de geração da chave pública, de cifração e decifração de mensagens são descritos a seguir.

II.2.2.1 - GERAÇÃO DA CHAVE PÚBLICA DE CIFRAR

No SCMH a chave pública de cifrar é obtida de acordo com o seguinte procedimento :

1º - Escolher uma seqüência $a' = (a'_1, a'_2, \ldots, a'_n)$ supercrescente de inteiros :

$$a'_i > \sum_{j=1}^{i-1} a'_j \quad , \quad i = 2,3,\ldots,n \qquad (II\text{-}1)$$
$$a'_1 > 0$$

Cada elemento a'_i deve escolhido aleatoriamente do intervalo definido por $[(2^{i-1} - 1).2^n + 1 \; ; \; 2^{i-1} . 2^n]$, onde $n \geq 100$.

2º - Escolher, aleatoriamente, dois números naturais w e M tais que :

$$M \in [2^{2n+1} + 1 \; ; \; 2^{2n+2} - 1]$$

$$M > \sum_{i=1}^{n} a'_i \qquad (II\text{-}2)$$

$$1 < w < M$$
$$(w,M) = 1 \qquad \text{(II-3)}$$

A condição (II-2) é necessária para a decifração única dos criptogramas, e os números w e M têm que ser primos entre si para assegurar que existe um valor w^{-1} mod M .

3º - Calcular o inverso de w módulo M , isto é, determinar w^{-1} tal que :

$$w \cdot w^{-1} \equiv 1 \pmod{M} \qquad \text{(II-4)}$$

4º - Gerar os elementos da chave de cifrar :

$$a_i = a'_i \cdot w \pmod{M} \qquad i = 1,2,\ldots,n \qquad \text{(II-5)}$$

onde :

$a = (a_i)_{i=1,n}$ é a chave de cifrar

$a' = (a'_i)_{i=1,n}$ é a chave de decifrar.

5º - Manter secretos os parâmetros w e M e a chave de decifrar:

$$a' = (a'_1, a'_2, \ldots, a'_n)$$

Tornar pública a chave de cifrar:

$$a = (a_1, a_2, \ldots, a_n)$$

(ou uma chave que seja permutação desta).

É esperado que a transformação modular (II-5) substitua o problema mochila fácil $(a'_i)_{i=1,n}$ pelo problema mochila $(a_i)_{i=1,n}$ difícil. Os parâmetros "trapdoor" secretos w e M devem ser escolhidos de forma que isso ocorra. (Se os parâmetros escolhidos gerarem um problema "fácil" - mochila

supercrescente, com elemento dominante ou outro tipo de seqüência fácil -, então os parâmetros devem ser trocados até que seja obtido um problema mochila "difícil"). Determinadas escolhas de w e M podem ser consideradas ruins, mesmo satisfazendo as condições (II-2) e (II-3) , se não gerarem mochilas difíceis. Por isso, o usuário do SCMH deve ficar atento à escolha desses parâmetros de modo a evitar que sejam geradas chaves públicas de cifrar "fáceis". Na literaura consultada, o problema de verificar se a mochila obtida após a multiplicação modular é "fácil" ou "difícil" não é abordado explicitamente.

A aplicação da multiplicação modular na geração do vetor mochila difícil $a = (a_1, a_2, \ldots, a_n)$ tem a finalidade de esconder a propriedade de supercrescimento do vetor mochila fácil $a' = (a'_1, a'_2, \ldots, a'_n)$ (para o qual existe um algoritmo linear em tempo para resolver o problema mochila associado) e, assim, prevenir a recuperação deste vetor por pessoas que não conheçam os parâmetros secretos **w** e **M** . No entanto, para qualquer pessoa que conheça esses parâmetros, a conversão do vetor $\mathbf{a} = (a_i)_{i=1,n}$ para o vetor $a' = (a'_i)_{i=1,n}$ torna-se trivial. De fato, com esses parâmetros, é muito fácil converter o problema mochila difícil, envolvendo o vetor **a** , em um problema mochila fácil, envolvendo o vetor **a'**.

II.2.2.2 - PROCESSO DE CIFRAÇÃO

Para cifrar uma mensagem no SCMH, o usuário deve proceder do seguinte modo:

1º - Converter o texto claro em uma cadeia de dígitos binários segundo uma representação previamente definida.

Por exemplo, cinco bits podem ser alocados para representar cada letra, número ou sinal de pontuação no texto claro, fornecendo um alfabeto de $2^5 = 32$ caracteres, com a seguinte representação binária :

A = 00000	B = 00001	C = 00010	D = 00011	E = 00100
F = 00101	G = 00110	H = 00111	I = 01000	J = 01001
K = 01010	L = 01011	M = 01100	N = 01101	O = 01110
P = 01111	Q = 10000	R = 10001	S = 10010	T = 10011
U = 10100	V = 10101	W = 10110	X = 10111	Y = 11000
Z = 11001	= 11010	. = 11011	, = 11100	? = 11101
; = 11110	: = 11111			

Em alguns criptossistemas é mais simples pensar em termos de um sistema não-binário, por exemplo um sistema decimal de 2 dígitos, permitindo representar até $10^2 = 100$ caracters, conforme :

a=00	b=01	c=02	d=03	e=04	f=05	g=06
h=07	i=08	j=09	k=10	l=11	m=12	n=13
o=14	p=15	q=16	r=17	s=18	t=19	u=20
v=21	w=22	x=23	y=24	z=25	A=26	B=27
C=28	D=29	E=30	F=31	G=32	H=33	I=34
J=35	K=36	L=37	M=38	N=39	O=40	P=41
Q=42	R=43	S=44	T=45	U=46	V=47	W=48
X=49	Y=50	Z=51	0=52	1=53	2=54	3=55
4=56	5=57	6=58	7=59	8=60	9=61	=62
.=63	,=64	;=65	?=66	...		

2º - Decompor a mensagem em blocos de n bits ou dígitos binários (sendo n o tamanho da chave de cifrar), formando n-plas binárias da forma :

$$x^{(j)} = (x_1^{(j)}, x_2^{(j)}, \ldots, x_n^{(j)}) \quad , \quad j = 1,2,\ldots,u$$

Se o último bloco da mensagem tiver menos que n dígitos, completar com zeros para obter-se a n-pla binária.

3º - Obter a chave de cifrar correspondente ao destinatário desejado. Esta chave de cifrar também tem a forma de uma n-pla, $a = (a_1, a_2, \ldots, a_n)$, onde cada elemento a_i é um inteiro positivo.

4º - Determinar o criptograma correspondente a cada bloco da mensagem, calculando o produto escalar :

$$S^{(j)} = \sum_{i=1}^{n} a_i . x_i^{(j)} = a . (x^{(j)})^T , \quad j=1,...,u \qquad (II-6)$$

onde : j é o índice identificador do bloco da mensagem,

$a = (a_1, ..., a_n)$ é a chave pública do destinatário desejado,

$x^{(j)} = (x_1^{(j)}, ... , x_n^{(j)})$ é a representação binária do j-ésimo bloco da mensagem.

5º - Enviar, ao destinatário desejado, os criptogramas $S^{(1)}$, $S^{(2)}, ..., S^{(u)}$.

Um interceptador defronta-se com a tarefa de recuperar $x^{(j)}$ a partir de $S^{(j)}$ e da chave pública de cifrar $a = (a_1, a_2, ..., a_n)$, que ele pode obter facilmente. Como cada elemento x_i é igual a 0 ou 1, a recuperação do bloco $x^{(j)}$ da mensagem a partir de $S^{(j)}$ equivale a resolver o problema mochila para o valor $S^{(j)}$ e o vetor $(a_i)_{i=1,n}$. O receptor deve resolver o mesmo problema mochila, mas sua tarefa é simplificada pelo conhecimento da informação "trapdoor".

A segurança do SCMH reside exatamente na dificuldade de um interceptador resolver o problema da mochila associado ao criptograma e à chave pública.

II.2.2.3 - PROCESSO DE DECIFRAÇÃO

Para decifrar a mensagem o receptor deve executar os seguintes passos :

1º - Calcular o criptograma transformado correspondente a cada criptograma $S^{(j)}$ recebido, usando os parâmetros secre - tos w^{-1} e M :

$$(S^{(j)})' = S^{(j)} . w^{-1} \pmod{M} \qquad \text{(II-7)}$$

Para todos os criptogramas transformados vale a análi se apresentada a seguir, e por isso o índice j será suprimi- do para clareza do texto.

$$S' \equiv S . w^{-1} \pmod{M}$$

$$S' \equiv w^{-1} . S \pmod{M}$$

$$S' \equiv w^{-1} . \sum_{i=1}^{n} a_i . x_i \pmod{M}$$

Como $x_i \bmod M = x_i$, e usando a equação (II-5) vem :

$$S' = w^{-1} . \sum_{i=1}^{n} (a'_i . w \bmod M) . x_i$$

$$S' = \sum_{i=1}^{n} (w^{-1} . w . a'_i \bmod M) . x_i$$

Pela equação (II-4) sabe-se que $w^{-1} . w \bmod M \equiv 1$, então :

$$S' = \sum_{i=1}^{n} a'_i . x_i \pmod{M} \qquad \text{(II-8)}$$

Como x_i é igual a 0 ou 1, e pela expressão (II-2) $M > \sum_{i=1}^{n} a'_i$, então a equação (II-8) torna-se :

$$S' = \sum_{i=1}^{n} a'_i . x_i \qquad \text{(II-9)}$$

2º - Recuperar todos os blocos $x^{(j)}$ da mensagem binária resolvendo, de modo trivial, o problema mochila associado à seqüência supercrescente, usando o resultado apresentado em (II-9) :

$$(S^{(j)})' = a' \cdot (x^{(j)})^T \quad , j=1,\ldots,u \qquad \text{(II-10)}$$

onde : $a' = (a'_1, a'_2, \ldots, a'_n)$ é a chave secreta do receptor (seqüência supercrescente),

$x^{(j)} = (x_1^{(j)}, x_2^{(j)}, \ldots, x_n^{(j)})$ é a seqüência binária que representa o j-ésimo bloco da mensagem ,

$(S^{(j)})'$ é o valor do criptograma transformado.

Desta forma, para decifrar o criptograma $S^{(j)}$ basta calcular o valor $S^{(j)} \cdot w^{-1} \bmod M$ e, então, resolver o problema mochila fácil associado, uma vez que o vetor $(a'_i)_{i=1,n}$ é supercrescente. O receptor simplesmente aplica seu vetor secreto $(a'_i)_{i=1,n}$ a fim de resolver o problema mochila para $(S^{(j)})'$ e recuperar $x = (x_1, x_2, \ldots, x_n)$.

Como o interceptador não conhece os parâmetros secretos w e M, ele não está apto, em princípio, a converter o criptograma para a forma na qual existe um algoritmo simples de decifração.

II.2.2.4 - EXEMPLO DE APLICAÇÃO

Os procedimentos descritos anteriormente ficarão mais claros com o exemplo simples apresentado em [4], e transcrito a seguir.

Seja uma mensagem em que a primeira palavra é HOW , cuja representação binária, utilizando-se um alfabeto binário de 5 dígitos, é : 00111011101011011010 (os últimos 5 bits correspondem ao espaço em branco entre a palavra HOW e a próxima palavra no texto).

Seja a chave pública de cifrar do receptor pretendido igual a :

a = (2292,1089,211,1625,1283,599,759,315,2597,2463)

O primeiro bloco de informação, o qual consiste nos 10 primeiros bits do texto claro binário, é :

x = (0, 0, 1, 1, 1, 0, 1, 1, 1, 0)

Este bloco será cifrado como :

$$S = a_1x_1 + a_2x_2 + \ldots + a_{10}x_{10}$$

$$S = (2292x0) + (1089x0) + (211x1) + (1625x1) + (1283x1) + (599x0) + (759x1) + (315x1) + (2597x1) + (2463x0)$$

$$S = 6790$$

Este valor é enviado ao destinatário pretendido.

Para decifrar este criptograma é necessário determinar quais elementos a_i fornecem a soma igual a 6790.

Neste exemplo, em que n = 10, o tamanho da chave pública é pequeno demais para prover segurança criptográfica ao sistema, permitindo a solução por exaustão em tempo razoável.

O receptor, ao gerar seu vetor público de cifrar $a = (a_i)_{i=1,10}$ começou escolhendo um vetor $a' = (a'_i)_{i=1,10}$ no qual cada elemento a'_i é maior que a soma dos elementos precedentes :

$$a' = (3,5,11,20,41,83,169,340,679,1358)$$

Para os valores $w = 764$ e $M = 2731$ ($w^{-1} = 1605$) , e aplicando a transformação modular (II-5), o receptor obteve o seu vetor chave de cifrar :

$$a_1 = 3 \times 764 \bmod 2731 = 2292$$

$$a_2 = 5 \times 764 \bmod 2731 = 1089$$

$$\vdots$$

$$a_{10} = 1358 \times 764 \bmod 2731 = 2463$$

O receptor, de posse do criptograma recebido $S = 6790$, calcula o criptograma transformado segundo (II-7) :

$$S' = S \cdot w^{-1} \bmod M$$

$$S' = 6790 \times 1605 \bmod 2731 = 1260$$

Outra vez o problema de decifrar é equivalente a resolver o problema mochila mas,neste caso, devido à propriedade especial do vetor $a' = (a'_i)_{i=1,10}$ (vetor supercrescente), o vetor-solução $x = (x_1, x_2, \ldots, x_{10})$ é facilmente determinado:

$$S' = a' \cdot x^T$$

$$1260 = 3x_1 + 5x_2 + 11x_3 + 20x_4 + 41x_5 + 83x_6 + 169x_7 + 340x_8 + 679x_9 + 1358\, x_{10}$$

Aplicando-se o algoritmo apresentado em II.1.2.1 , recupera-se o vetor $x = (x_1, x_2, \ldots, x_{10})$ correspondente ao primeiro bloco da mensagem original :

$$x = (0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$$

II.2.3 - MÉTODO DE ITERAÇÃO MÚLTIPLA

Com a finalidade de aumentar a segurança e utilidade do método básico, MERKLE e HELLMAN [3] propuseram o método de iteração múltipla.

O método iterativo é uma variante do método de iteração simples, e consiste, basicamente, na utilização de transformações modulares sucessivas para geração do vetor chave de cifrar.

Espera-se que a transformação modular definida em (II-5) converta um problema mochila fácil, envolvendo o vetor supercrescente $a' = (a'_1 , a'_2 , \ldots , a'_n)$, em um problema mochila difícil, envolvendo o vetor $a = (a_1 , a_2 , \ldots , a_n)$. Este processo pode ser repetido, tantas vezes quantas forem desejadas, para produzir vetores cujo problema mochila associado parece muito mais difícil. Em cada transformação modular sucessiva, empregando-se os parâmetros (w_1, M_1), (w_2, M_2), etc, espera-se que a estrutura do vetor obtido torne-se mais e mais obscura. O resultado final, vetor público de cifrar, parece ser um conjunto de números aleatórios, e o fato de o problema original ser facilmente resolvido foi camuflado.

Vale mencionar que a transformação total não é, em geral, equivalente a uma única transformação (w,M), como mostrado em [3] :

Seja o vetor supercrescente $a^{(1)} = (5, 10, 20)$ e sejam adotados os seguintes parâmetros :

$$w_1 = 17 \quad , \quad M_1 = 47$$

$$w_2 = 3 \quad , \quad M_2 = 89$$

Aplicando a primeira transformação (w_1, M_1) obtém-se:

$$a_i^{(2)} = a_i^{(1)} \cdot w_1 \bmod M_1 \quad , \quad i = 1,2,3$$

$$a_1^{(2)} = (5 \times 17) \bmod 47 = 38$$

$$a_2^{(2)} = (10 \times 17) \bmod 47 = 29$$

$$a_3^{(2)} = (20 \times 17) \bmod 47 = 11$$

$$a^{(2)} = (38, 29, 11)$$

Aplicando a segunda transformação (w_2, M_2) vem :

$$a_i^{(3)} = a_i^{(2)} \cdot w_2 \bmod M_2 \quad , \quad i = 1,2,3$$

$$a_1^{(3)} = (38 \times 3) \bmod 89 = 25$$

$$a_2^{(3)} = (29 \times 3) \bmod 89 = 87$$

$$a_3^{(3)} = (11 \times 3) \bmod 89 = 33$$

$$a^{(3)} = (25, 87, 33)$$

(Observe-se que esta seqüência é supercrescente permutada.)

Supondo que existam $\hat{w}$ e $\hat{M}$ tais que :

$$a_i^{(3)} = a_i^{(1)} \cdot \hat{w} \bmod \hat{M} \quad , \quad i = 1,2,3$$

pode-se escrever :

$$i = 1 \rightarrow 25 = 5 \cdot \hat{w} \bmod \hat{M}$$

$$i = 2 \rightarrow 87 = 10 \cdot \hat{w} \bmod \hat{M}$$

Multiplicando a primeira expressão por 2 e efetuando a diferença em relação à segunda vem :

$$50 = 10 \cdot \hat{w} \bmod \hat{M}$$

$$87 = 10 \cdot \hat{w} \bmod \hat{M}$$

$$37 = 0 \bmod \hat{M} \qquad \therefore \qquad \hat{M} = 37$$

Substituindo este valor na equação correspondente ao primeiro elemento da mochila obtém-se :

$$25 = 5 \cdot \hat{w} \mod 37 \qquad \therefore \qquad \hat{w} = 5$$

Aplicando os valores $\hat{w} = 5$ e $\hat{M} = 37$ para o terceiro elemento do vetor tem-se :

$$a_3^{(3)} = a_3^{(1)} \cdot \hat{w} \mod \hat{M}$$

$$33 = (20 \times 5) \mod 37$$

mas,

$$100 \mod 37 = 26$$

e portanto,

$33 = 26 \mod 37$ é uma contradição.

Logo, conclui-se que não existem $\hat{w}$ e $\hat{M}$ que satisfaçam o problema da transformação.

No método de iteração múltipla proposto por MERKLE e HELLMAN [3] é utilizado, como vetor inicial, um vetor mochila supercrescente $a' = (a'_1 , a'_2 , \ldots , a'_n)$. Esta mochila fácil é então "camuflada" por k iterações de multiplicação modular para produzir um vetor mochila alçapão (com passagem secreta) $a = (a_1 , a_2 , \ldots , a_n)$, o qual é, em geral, difícil e utilizado como chave pública de cifrar.

II.2.3.1 - GERAÇÃO DA CHAVE PÚBLICA DE CIFRAR

O algoritmo para obtenção da chave de cifrar é composto pelos seguintes passos :

1º - Escolher uma seqüência $a_0 = (a_{0,1} , a_{0,2} , \ldots , a_{0,n})$ de inteiros, tal que :

$$a_{0,i} > \sum_{j=1}^{i-1} a_{0,j} \quad , \quad i = 2,\ldots,n \qquad \text{(II-11)}$$

$$a_{0,1} > 0$$

2º - Gerar inteiros positivos w_1 e M_1 tais que :

$$M_1 > \sum_{i=1}^{n} a_{0,i} \qquad \text{(II-12)}$$

$$1 < w_1 < M_1 \qquad \text{(II-13)}$$

$$(w_1 , M_1) = 1$$

3º - Determinar o inverso de w_1 módulo M_1 tal que :

$$w_1 \cdot w_1^{-1} \equiv 1 \pmod{M_1} \qquad \text{(II-14)}$$

$$0 < w_1^{-1} < M_1$$

4º - Calcular os elementos da seqüência modificada :

$$a_{1,i} \equiv a_{0,i} \cdot w_1 \bmod M_1 \quad , \quad i = 1,\ldots,n \qquad \text{(II-15)}$$

.
.
.

(Repetir os 2º, 3º e 4º passos quantas vezes desejar.)

Para uma iteração genérica k , tem-se :

(3k-1)º - Gerar inteiros positivos w_k e M_k tais que :

$$M_k > \sum_{i=1}^{n} a_{k-1,i} \qquad \text{(II-16)}$$

$$1 < w_k < M_k$$
$$(w_k, M_k) = 1 \qquad \text{(II-17)}$$

(3k)º - Determinar o inverso de w_k módulo M_k tal que :

$$w_k \cdot w_k^{-1} \equiv 1 \pmod{M_k}$$
$$0 < w_k^{-1} < M_k \qquad \text{(II-18)}$$

(3k+1)º - Gerar os elementos da chave de cifrar :

$$a_{k,i} \equiv a_{k-1,i} \cdot w_k \bmod M_k \quad , \quad i = 1,\ldots,n \qquad \text{(II-19)}$$

ÚLTIMO PASSO - Definir uma permutação para os elementos da seqüência $(a_{k,i})_{i=1,n}$ e publicar a seqüencia $(a_i)_{i=1,n}$ obtida :

Chave pública de cifrar :

$$a = (a_1, a_2, \ldots, a_n)$$

Chave secreta :

$$a_0 = (a_{0,1}, a_{0,2}, \ldots, a_{0,n})$$

Parâmetros secretos :

$$((w_1,M_1), (w_2,M_2), \ldots, (w_k,M_k))$$

Deve-se tomar cuidado com a taxa de crescimento do vetor $a = (a_i)_{i=1,n}$ pois esta taxa determina a expansão de dados envolvida na transmissão da mensagem. Esta taxa de crescimento depende do método de escolha dos parâmetros [3].

II.2.3.2 - PROCESSO DE CIFRAÇÃO

O processo de cifração de uma mensagem no método de iteração múltipla é idêntico àquele descrito no método básico apresentado no item II.2.2.2 .

II.2.3.3 - PROCESSO DE DECIFRAÇÃO

Para decifrar a mensagem, o receptor deve executar os seguintes passos :

1º - Obter, para cada criptograma recebido $S_k^{(j)}$, o criptograma transformado correspondente ao vetor mochila supercrescente, utilizando as transformações modulares inversas sucessivas :

$$\begin{aligned} S_{k-1}^{(j)} &\equiv S_k^{(j)} \cdot w_k^{-1} \bmod M_k \\ &\vdots \qquad\qquad , \quad j = 1,2,\ldots,u \\ S_0^{(j)} &\equiv S_1^{(j)} \cdot w_1^{-1} \bmod M_1 \end{aligned} \tag{II-20}$$

2º - Recuperar todos os blocos $x^{(j)}$ da mensagem binária resolvendo o problema mochila associado à mochila supercrescente :

$$S_0^{(j)} = \sum_{i=1}^{n} a_{0,i} \cdot x_i^{(j)} \tag{II-21}$$

onde : $a_0 = (a_{0,1}, \ldots, a_{0,n})$, vetor secreto de decifrar, é uma seqüência supercrescente ;

$x^{(j)} = (x_1^{(j)}, \ldots, x_n^{(j)})$ é a seqüência binária que representa o j-ésimo bloco da mensagem;

$S_0^{(j)}$ é o criptograma correspondente à mochila supercrescente.

II.2.3.4 - EXEMPLO DE APLICAÇÃO

Os valores usados neste exemplo são pequenos demais para prover segurança a um sistema criptográfico, mas servem para ilustrar o método de iteração múltipla :

1º - Geração da chave pública de cifrar : $n = 4$ e $k = 3$

Seja a mochila supercrescente $a_0 = (2, 3, 6, 12)$.

Para esta seqüência podem ser adotados :

$$M_1 = 25 \quad (> 2 + 3 + 6 + 12 = 23)$$

$$w_1 = 14 \qquad \therefore \qquad w_1^{-1} \bmod 25 = 9$$

Usando estes valores obtém-se :

$$a_{1,i} = w_1 \cdot a_{0,i} \bmod M_1 \quad , \quad i = 1,2,3,4$$

$$a_1 = (3, 17, 9, 18)$$

Para esta seqüência podem ser adotados :

$$M_2 = 101 \quad (> 3 + 17 + 9 + 18 = 47)$$

$$w_2 = 64 \qquad \therefore \qquad w_2^{-1} \bmod 101 = 30$$

Assim :

$$a_{2,i} = w_2 \cdot a_{1,i} \bmod M_2 \quad , \quad i = 1,2,3,4$$

$$a_2 = (91, 78, 71, 41)$$

Escolhendo:

$$M_3 = 301 \quad (> 91 + 78 + 71 + 41 = 281)$$

$$w_3 = 16 \qquad \therefore \qquad w_3^{-1} \bmod 301 = 207$$

Calcula-se :

$$a_{3,i} = w_3 \cdot a_{2,i} \bmod M_3 \quad , \quad i = 1,2,3,4$$

$$a_3 = (252, 44, 233, 54)$$

que é a chave pública de cifrar.

2º - Cifração da mensagem :

Seja $x = (1, 1, 0, 1)$ a mensagem a ser enviada. Então o criptograma será :

$$S_3 = \sum_{i=1}^{4} a_{3,i} \cdot x_i = 252 + 44 + 54 = 350$$

3º - Decifração do criptograma :

Aplicando as transformações modulares secretas sobre o criptograma S_3 obtém-se :

$$S_{k-1} = S_k \cdot w_k^{-1} \bmod M_k \quad , \quad k = 3,2,1$$

$$S_2 = (350 \times 207) \bmod 301 = 210$$

$$S_1 = (210 \times 30) \bmod 101 = 38$$

$$S_0 = (38 \times 9) \bmod 25 = 17$$

$$S_0 = \sum_{i=1}^{4} a_{0,i} \cdot x_i = 17$$

Como o vetor $a_0 = (2, 3, 6, 12)$ é supercrescente, a recuperação do vetor $x = (x_1, x_2, x_3, x_4)$ é trivial :

$$x = (1, 1, 0, 1)$$

II.2.4 - MÉTODO DA MOCHILA MULTIPLICATIVA

O problema da mochila multiplicativa consiste em determinar os elementos de um conjunto que, multiplicados, fornecem um valor especificado. Uma condição para solução fácil de uma mochila multiplicativa é que seus elementos sejam primos entre si.

Um vetor mochila multiplicativo, apresentando uma solução fácil, pode ser transformado em um vetor mochila aditivo, com solução difícil, tomando-se logaritmos. Para assegurar que ambos os vetores (aditivo e multiplicativo) terão valores razoáveis, o logaritmo é considerado sobre GF(p), onde p é um número primo.

MERKLE e HELLMAN [3] utilizaram esses conceitos para desenvolver o método criptográfico de chave pública baseado na mochila multiplicativa, cuja descrição formal é apresentada a seguir.

II.2.4.1 - GERAÇÃO DA CHAVE PÚBLICA DE CIFRAR

Para obtenção da chave pública de cifrar devem ser efetuados os seguintes passos :

1º - Escolher um vetor "trapdoor" $a' = (a'_1, a'_2, \ldots, a'_n)$ tal que os elementos a'_i sejam primos entre si.

2º - Determinar o parâmetro M tal que :

$$M > \prod_{i=1}^{n} a'_i \qquad \text{(II-22)}$$

3º - Escolher uma base b para cálculo dos logaritmos, tal que $b > 0$, inteiro qualquer.

4º - Calcular o logaritmo na base b módulo M , de cada elemento do vetor $a' = (a'_1, a'_2, \ldots, a'_n)$:

$$a_i = \log_b a'_i \pmod{M} \quad , \quad i = 1,\ldots,n \qquad \text{(II-23)}$$

que corresponde, na operação inversa :

$$(b)^{a_i} = a'_i \pmod{M} \quad , \quad i = 1,\ldots,n \qquad \text{(II-24)}$$

onde : $a' = (a'_1 ,\ldots, a'_n)$ é o vetor mochila multiplicativo;

$a = (a_1 ,\ldots, a_n)$ é o vetor mochila aditivo.

5º - Chave secreta :

$$a' = (a'_1, a'_2, \ldots, a'_n)$$

Parâmetros secretos : b e M

Chave pública :

$$a = (a_1, a_2, \ldots, a_n)$$

II.2.4.2 - PROCESSO DE CIFRAÇÃO

Para cifrar uma mensagem no método da mochila multiplicativa, deve-se proceder como em II.2.2.2 .

II.2.4.3 - PROCESSO DE DECIFRAÇÃO

Para decifrar os criptogramas recebidos e, então, recuperar o texto claro, o receptor deve executar o seguinte procedimento :

1º - Determinar o criptograma transformado, correspondente a cada criptograma recebido, efetuando :

$$(S^{(j)})' = (b)^{S^{(j)}} \bmod M \quad , \quad j = 1,\ldots,u \qquad \text{(II-26)}$$

Usando a equação (II-26) e suprimindo o índice j , pode-se escrever :

$$S' = (b)^{\left(\sum_{i=1}^{n} a_i . x_i\right)} \bmod M$$

$$S' = \prod_{i=1}^{n} (b)^{(a_i . x_i)} \bmod M$$

$$S' = \prod_{i=1}^{n} (b^{a_i})^{x_i} \bmod M$$

$$S' = \prod_{i=1}^{n} (a_i')^{x_i} \bmod M \qquad \text{(II-27)}$$

Como $M > \prod_{i=1}^{n} a_i'$ pela expressão (II-22) e x_i é 0 ou 1 , então a equação (II-27) pode ser escrita como :

$$S' = \prod_{i=1}^{n} (a_i')^{x_i} \qquad \text{(II-28)}$$

2º - Recuperar todos os blocos $x^{(j)}$ da mensagem binária resolvendo o problema mochila fácil associado ao vetor multiplicativo $a' = (a'_1, a'_2, \ldots, a'_n)$, usando o resultado obtido em (II-28) :

$$(S^{(j)})' = \prod_{i=1}^{n} (a'_i)^{x_i^{(j)}} \quad , \quad j = 1,\ldots,u \qquad \text{(II-29)}$$

onde : $a' = (a'_1 ,\ldots, a'_n)$ é o vetor multiplicativo fácil, considerado como chave secreta de decifrar;

$x^{(j)} = (x_1^{(j)},\ldots, x_n^{(j)})$ é a seqüência binária que representa o j-ésimo bloco da mensagem;

$(S^{(j)})'$ é o criptograma transformado, associado ao vetor multiplicativo.

Como os elementos do vetor $a' = (a'_i)_{i=1,n}$ são primos entre si, para obter o vetor binário (que representa o j-ésimo bloco da mensagem) $x^{(j)} = (x_i^{(j)})_{i=1,n}$ com facilidade, basta dividir $(S^{(j)})'$ por a'_i , para $i = 1,n$, verificando quais elementos foram utilizados na multiplicação para formar o número $(S^{(j)})'$: se o resultado da divisão for um inteiro, então $x_i = 1$, caso contrário $x_i = 0$.

Um interceptador que conheça a chave pública (vetor $a = (a_i)_{i=1,n}$) mas que não conheça as informações secretas "trapdoor" M e b , se deparará, em geral, com um problema computacional difícil.

No método da mochila multiplicativa, o grau de expansão de dados (definido em II.2.5) é muito elevado e, por esta razão, os sistemas mochila multiplicativos não são considerados para aplicações práticas em sistemas criptográficos, e também porque um sistema multiplicativo pode ser transformado em um sistema aditivo clássico.

II.2.4.4 - EXEMPLO DE APLICAÇÃO

Sejam : $n = 4$

$M = 257$

$b = 131$

$a' = (2, 3, 5, 7)$

Calculando o vetor público segundo (II-23) obtém-se:

$$a = (80, 183, 81, 195)$$

Seja o seguinte vetor mensagem binário :

$$x = (0, 1, 1, 0) ,$$

que fornece o criptograma :

$$S = 183 + 81 = 264 .$$

O receptor autorizado deseja obter o vetor mensagem a partir desse criptograma. Como ele conhece as informações secretas "trapdoor" M e b , pode então calcular :

$$S' = b^S \bmod M$$

$$S' = 131^{264} \bmod 257$$

$$S' = 15$$

Resta saber que elementos do vetor secreto (conhecido pelo receptor autorizado) foram multiplicados para fornecer $S' = 15$.

Pode-se escrever :

$$S' = 15 = 2^{x_1} \cdot 3^{x_2} \cdot 5^{x_3} \cdot 7^{x_4}$$

Assim, os elementos x_i são facilmente determinados :

$15 \div 2 = 7,5 \rightarrow x_1 = 0$

$15 \div 3 = 5 \rightarrow x_2 = 1$

$15 \div 5 = 3 \rightarrow x_3 = 1$

$15 \div 7 = 2,14 \rightarrow x_4 = 0$

Portanto a mensagem é : $x = (0, 1, 1, 0)$

II.2.5 - VANTAGENS E DESVANTAGENS DO SCMH

O SCMH apresenta as seguintes vantagens :

1ª - Distribuição de Chaves

Um dos maiores problemas no projeto de um sistema criptográfico para comunicação segura é prover a adequada distribuição de chaves aos emissores e receptores das mensagens cifradas. As chaves devem ser produzidas e distribuídas não apenas uma vez, mas constantemente. Em alguns sistemas elas devem ser trocadas com o passar do tempo ou após uma determinada quantidade de tráfego de mensagens, e em todos os sistemas elas devem ser trocadas sempre que forem comprometidas.

Até o momento, a criptografia de chave pública parece ser a solução mais satisfatória e elegante para o problema de distribuição de chaves. A principal vantagem dos criptossistemas de chave pública é a não necessidade de distribuição prévia das chaves entre os comunicadores (usuários do sistema) utilizando-se um canal seguro (e caro) mas, ao contrário, essas chaves podem ser divulgadas até mesmo numa lista pública. Isso é possível porque, para cada usuário, as chaves de cifrar e de decifrar são diferentes e, conhecendo-se apenas a chave pública (chave de cifrar) é muito difícil obter a chave secreta (chave de decifrar) sem o conhecimento da informação "trapdoor". (Permanece, no entanto, o problema de um usuário se fazer passar por outro, isto é, um impostor.)

2ª - Implementação fácil e processos rápidos

Outra vantagem do sistema criptográfico tipo mochila é que exige pequeno esforço computacional para executar todas as operações envolvidas, e, consequentemente, sua implementação é fácil. Neste sistema as chaves podem ser geradas rapidamente. O processo de cifração de uma mensagem binária de n

bits consiste em, no máximo, n operações de adição e a decifração envolve não mais que n multiplicações e aproximadamente o mesmo número de subtrações. Assim sendo, o sistema oferece alta velocidade para as operações de cifrar e de decifrar. Até mesmo para o método de iteração múltipla essas operações são muito rápidas.

Para aumentar ainda mais a velocidade de decifração no sistema criptográfico de chave pública tipo mochila, HENRY [16] propôs um algoritmo simples, cuja descrição detalhada é apresentada na referência.

Como desvantagens do SCMH podem ser citadas :

1ª - Expansão de dados

A expansão de dados é definida como sendo a relação entre o número de bits no criptograma e o número de bits no bloco correspondente da mensagem, ou ainda, em termos percentuais, como sendo a diferença : 1 (um) menos o valor desta relação.

A expansão de dados é uma grande desvantagem dos criptossistemas tipo mochila, quase dobrando a quantidade de dados a ser transmitida, mas tal desvantagem pode ser aceitável. A assinatura digital é um requisito importante para comunicações seguras. No entanto, devido à expansão de dados , sistema criptográfico de chave pública tipo mochila não é muito eficiente para produzir assinaturas de mensagens.

2ª - Tamanho da chave pública

Outra desvantagem do sistema de Merkle-Hellman é o tamanho, em bits, da chave pública, podendo atingir algumas dezenas de milhares de bits (normalmente maior que 10.000 bits = 100 elementos x 100 bits por elemento da chave pública). Esse fato acarreta um problema em termos de memória ne

cessária para armazenar todas as chaves públicas nos sistemas de usuário.

Uma maneira possível de reduzir o tamanho da chave pública (enquanto mantendo o conjunto original de mensagens) é reduzir o tamanho n do vetor de cifrar e permitir soluções não binárias para o vetor mensagem. Esta formulação foi proposta por AMIRAZIZI et alii [14], e denominada de "mochila compacta", uma vez que permite a redução da chave cifrando mensagens não-binárias. A mochila compacta foi sugerida como uma forma prática de reduzir o tamanho da chave pública mantendo, no entanto, a mesma segurança propiciada pela mochila binária correspondente.

3ª - Segurança questionada

No Capítulo III são apresentados os ataques criptoanalíticos aplicáveis ao SCMH, evidenciando as vulnerabilidades criptográficas deste sistema.

CAPÍTULO III

MÉTODOS DE ATAQUE AO CRIPTOSSISTEMA MOCHILA DE CHAVE PÚBLICA

III.1 - CONSIDERAÇÕES INICIAIS

Desde o aparecimento da criptografia de chave pública , introduzida em 1976 por DIFFIE e HELLMAN [1], muitos estudiosos se preocuparam em formular criptossistemas de chave pública para prover comunicação segura entre os usuários de um sistema. Primeiramente RIVEST,SHAMIR e ADLEMAN [2] desenvolveram um sistema criptográfico baseado na Teoria dos Números (Sistema RSA). Logo depois, MERKLE e HELLMAN [3] apresentaram o seu criptossistema baseado no algoritmo da mochila. A partir de então muitas variantes, e mesmo novos criptossistemas de chave pública, foram propostos mas, por várias razões, os dois primeiros sistemas continuaram a dominar o campo e, por isso mesmo, têm sido extensamente analisados.

Como este trabalho se restringe ao estudo das aplicações criptográficas do algoritmo da mochila, serão discutidos apenas os ataques criptoanalíticos relativos ao sistema de chave pública tipo mochila.

Existem várias razões para se suspeitar da segurança do criptossistema de Merkle-Hellman. Uma delas é a exigência de que os elementos da mochila fácil (chave secreta) sejam supercrescentes. Esta estrutura se constitui numa informação que pode ser explorada pelo criptoanalista. Por outro lado, todos os esquemas mochila são aditivos no sentido de que o criptograma da soma é igual à soma dos criptogramas e, apesar de não se saber ainda como explorar esta propriedade num ataque criptoanalítico, a aditividade por si só é uma restrição severa.

Vários pesquisadores têm se preocupado em avaliar a segurança do sistema criptográfico de chave pública tipo mochila , ressaltando as suas vulnerabilidades criptoanalíticas. Vale mencionar que, paralelamente, têm sido desenvolvidas e apresentadas por outros estudiosos contramedidas para tornar o sistema mochila mais seguro às investidas criptoanalíticas, assunto que será discutido no próximo capítulo.

III.2 - MÉTODOS DE ATAQUE

A criptoanálise é a busca de maneiras de comprometer os sistemas de comunicações secretas. Por isso mesmo, a segurança da maioria dos sistemas criptográficos reside na dificuldade computacional para o criptoanalista descobrir o texto claro sem o conhecimento da chave de decifrar.

Nos sistemas criptográficos de chave pública tipo mochila a criptoanálise pode ser realizada, basicamente, segundo uma das formas:

1º - Recuperando, primeiramente, a chave secreta (informação "trapdoor") para depois , então, obter a mensagem em texto claro;

2º - Recuperando o texto claro diretamente:

i) por meio de ataque aos criptogramas,

ii) manipulando-se os elementos da chave pública,

iii) explorando as características e propriedades do sistema criptográfico,

iv) ou uma combinação desses modos.

Segundo este enfoque, os ataques encontrados na literatura, a partir de um levantamento bibliográfico extenso, foram agrupados em classes correlatas, conforme apresentado a seguir.

III.2.1 - EXAUSTÃO OU FORÇA BRUTA

A mais antiga forma de tentativa de quebra de um sistema criptográfico - a exaustão ou força bruta, também pode ser empregada contra o sistema criptográfico de chave pública tipo mochila.

A exaustão é a forma mais rudimentar de criptoanálise , sendo atualmente ainda empregada em muitos casos, quando não se dispõem de métodos mais elaborados ou então quando sua utilização for obrigatória por alguma outra razão.

A idéia básica desse tipo de ataque é recuperar a mensagem a partir do conhecimento do criptograma apenas, testando-se "todas" as possíveis mensagens para descobrir aquela que gerou o criptograma sob análise.

É sabido que o problema geral da mochila é NP-completo, e o tempo de processamento computacional necessário para obter a solução por tentativa cresce exponencialmente com o tamanho do problema. (Para um criptossistema mochila em que a mensagem original é binária e a chave de cifrar é de tamanho n, o interceptador tem que procurar pela mensagem entre as 2^n possibilidades).

Para evitar, ou pelo menos dificultar, a criptoanálise por exaustão,é preciso que o tamanho da mochila seja tal que torne a análise das diversas tentativas possíveis uma tarefa praticamente inviável ($n \geq 100$).

Em termos práticos , a utilização dessa forma de criptoanálise se restringe aos casos em que o tamanho do sistema ainda permite a recuperação da informação desejada num tempo computacional viável.

III.2.2 - RECUPERAÇÃO DA CHAVE SECRETA

III.2.2.1 - CONSIDERAÇÕES

Nesta classe de ataque estão as técnicas que, utilizando o conhecimento da estrutura de construção da chave de cifrar (isto é, as características e propriedades do sistema criptográfico tipo mochila), analisam os elementos da chave pública (e não os criptogramas) para recuperar a informação "trapdoor" e, então, obter a chave de decifrar, ou chave secreta.

A informação "trapdoor" é o par de valores representado pelos parâmetros w (multiplicador) e M (módulo) usados para esconder a característica de supercrescimento dos elementos da chave secreta. Essa informação é mantida em segredo, uma vez que seu conhecimento possibilita a obtenção da chave secreta a partir da chave pública, tornando trivial a recuperação da mensagem.

Há necessidade de manter secretos os dois parâmetros w e M pois, segundo SHAMIR e ZIPPEL [13], " o conhecimento de um dos parâmetros da transformação modular, mais precisamente o valor do módulo M, permite ao criptoanalista quebrar, em tempo polinomial, o esquema de Merkle-Hellman". Por isso, só serão apresentados neste capítulo os ataques para o caso em que os dois parâmetros são mantidos em segredo.

O criptossistema de Merkle-Hellman pode ser de iteração simples (utilizando apenas uma transformação modular - um par w, M) ou de iteração múltipla (utilizando vários pares w_j, M_j).

Como mostrado por MERKLE-HELLMAN [3], uma transformação modular única não é, em geral, equivalente a uma transformação modular múltipla. Por isso, as técnicas de criptoanálise dos sistemas de iteração simples são diferentes daquelas aplicáveis aos sistemas de iteração múltipla.

A seguir são apresentadas e avaliadas as técnicas de ataque criptoanalítico aos sistemas mochila de iteração simples e de iteração múltipla.

III.2.2.2 - MOCHILA DE ITERAÇÃO SIMPLES

III.2.2.2.1 - INTRODUÇÃO

O primeiro ataque criptoanalítico contra mochilas de iteração simples foi apresentado em 1981 por EIER e LAGGER [25]. A idéia básica do esquema é determinar pares de números naturais, isto é, valores para o módulo M e para o multiplicador w, os quais reduzem, simultaneamente, os elementos da mochila pela multiplicação modular, e selecionar aquele par que satisfaz as condições impostas no criptossistema de Merkle-Hellman.

Em abril de 1982, SHAMIR [27], usando técnicas de Programação Matemática, apresentou um algoritmo mais elaborado para quebrar, em tempo polinomial, a variante de iteração simples do sistema de Merkle-Hellman. A sua técnica se propõe a determinar algum par "trapdoor" w, M (mas não é garantido encontrar o par original) de forma que a seqüência transformada seja supercrescente e a soma de seus elementos seja menor do que M.

No mesmo ano, BRICKELL e SIMMONS [29], procederam a uma análise profunda do método de ataque desenvolvido por SHAMIR [27] e propuseram uma técnica de criptoanálise que se constitui numa versão melhorada do algoritmo descrito em [27], utilizando os mesmos conceitos básicos.

Em todos esses casos a idéia central do algoritmo de quebra é descobrir uma informação "trapdoor" (não necessariamente os parâmetros secretos usados na transformação modular original) para depois, então, recuperar o texto claro.

A seguir são descritas as características gerais de algumas técnicas encontradas na literatura para ataque ao sistema mochila de iteração simples.

III.2.2.2.2 - CARACTERÍSTICAS DAS TÉCNICAS DE ATAQUE

III.2.2.2.2.1 - TÉCNICA DE EIER-LAGGER

A idéia básica da técnica de ataque proposta por EIER e LAGGER [25] é analisar os elementos da chave pública, conhecendo as características de construção do criptossistema de Merkle e Hellman, para determinar pares de números naturais $\bar{M}$ e $\bar{w}$ (isto é, valores para o módulo e o multiplicador) os quais reduzem simultaneamente os elementos da mochila, por meio da multiplicação modular, a uma seqüência supercrescente e, assim, tornar possível a criptoanálise de qualquer criptograma.

O criptoanalista não conhece o par M, w usado na transformação modular original. Entretanto, ele pode tentar encontrar outros pares de números naturais $\bar{M}$ e $\bar{w}$ ($\bar{w} < \bar{M}$), que satisfazem às seguintes propriedades:

$$\bar{a}'_i = a_i \cdot \bar{w} \pmod{\bar{M}} \quad , \quad i=1,\ldots,n \qquad \text{(III-1)}$$

$$\sum_{i=1}^{n} \bar{a}'_i < \bar{M} \qquad \text{(III-2)}$$

O problema desse tipo de análise é encontrar pares apropriados de números naturais $\bar{M}$ e $\bar{w}$, os quais reduzem os elementos a_i simultaneamente por multiplicação modular. Segundo SHAMIR e ZIPPEL [13], a probabilidade de que dois números aleatoriamente escolhidos tenham essa propriedade é muito pequena. Desta forma, o conhecimento de um par correto de inteiros $\bar{M}$ e $\bar{w}$ é quase equivalente ao conhecimento da informação "trapdoor" original.

Proceder a uma busca exaustiva para determinar os parâmetros corretos $\bar{M}$ e $\bar{w}$ parece ser computacionalmente inviável. Para reduzir o número de candidatos possíveis, primeiramente estuda-se o efeito da operação expressa em (III-1), a qual pode ser escrita de forma equivalente como:

$$\frac{\bar{a}_i'}{\bar{M}} = a_i \cdot \frac{\bar{w}}{\bar{M}} \pmod 1 \qquad \text{(III-3)}$$

ou ainda fazendo $\bar{V} = \bar{w} / \bar{M}$, e portanto $0 < \bar{V} < 1$ é um número racional, vem :

$$\frac{\bar{a}_i'}{\bar{M}} = a_i \cdot \bar{V} \pmod 1 \qquad \text{(III-4)}$$

cuja representação gráfica é :

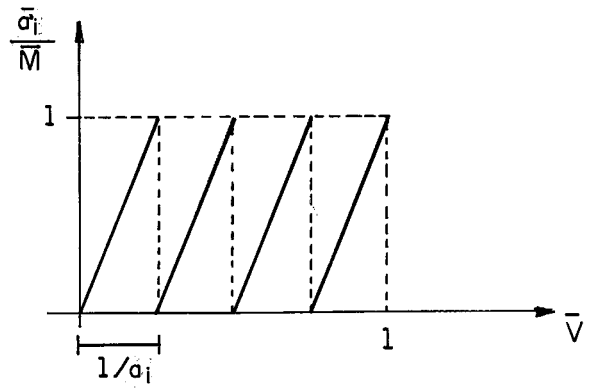


FIGURA III-1 : VARIAÇÃO DO VALOR $\bar{a}_i'/\bar{M}$ EM FUNÇÃO DE $\bar{V}$.

Nesta curva, a inclinação das linhas paralelas é a_i , o período da curva dente-de-serra é $1/a_i$, e o maior valor alcançado pelo gráfico é 1 (em ambas as coordenadas).

Como mencionado anteriormente, o criptoanalista tem que determinar pares de números naturais $\bar{M}$ e $\bar{w}$ que satisfaçam à propriedade:

$$\sum_{i=1}^{n} a_i \cdot \bar{V} \pmod 1 \; < \; 1 \qquad \text{(III-5)}$$

[Lembrar que $\sum_{i=1}^{n} \bar{a}_i' < \bar{M} \quad \therefore \quad \sum_{i=1}^{n} \bar{a}_i' / \bar{M} < 1$]

Isto significa que o criptoanalista precisa determinar um parâmetro racional $\bar{V}$ em vez de dois parâmetros $\bar{M}$ e $\bar{w}$.

Se todas as curvas dente-de-serra com período $1/a_i$ forem somadas, a curva resultante será, em geral, maior que 1. Deve, entretanto, existir pelo menos um intervalo pequeno $[V_1,V_2]$ onde esta função resultante é menor que 1. Uma vez que este intervalo tenha sido encontrado, não existe dificuldade para se determinar números naturais $\bar{M}$ e $\bar{w}$ cuja razão $\bar{V}=\bar{w}/\bar{M}$ esteja no intervalo $V_1 < \bar{V} < V_2$. De posse dos valores $\bar{M}$ e $\bar{w}$ (informação "trapdoor"), e conhecida a chave pública de cifrar, o criptoanalista pode determinar uma chave de decifrar e, então, facilmente recuperar qualquer vetor mensagem $x=(x_i)_{i=1,n}$ binário.

Observa-se que a propriedade de supercrescimento dos elementos da mochila $(a_i)_{i=1,n}$ não foi considerada explicitamente no método de criptoanálise descrito acima, tendo sido considerada apenas a propriedade de tamanho na equação (III-5). Obtidos os valores de $\bar{M}$ e $\bar{w}$ a partir da determinação de $\bar{V}$, basta realizar a transformação modular expressa em (III-1) para verificar se os elementos $\bar{a}'_i$ são supercrescentes. Em caso negativo, repetir o processo até determinar um par "trapdoor" tal que a seqüência transformada satisfaça as condições de tamanho e supercrescimento.

III.2.2.2.2.2 - TÉCNICA DE SHAMIR

A técnica de ataque criptográfico ao sistema de chave pública de Merkle-Hellman proposta por SHAMIR [27] se propõe a determinar algum par "trapdoor" M, w (mas não é garantido encontrar o par original) de forma que a seqüência transformada seja supercrescente, e com a restrição de que a soma de seus elementos seja menor do que M.

Uma vez determinados os valores de w e M, facilmente pode ser resolvido o problema mochila associado e, então, o texto claro correspondente a qualquer criptograma gerado pode ser obtido com facilidade.

Em seu artigo SHAMIR [27] apresenta uma extensa descrição do algoritmo proposto, no qual o ponto fundamental é a representação gráfica da construção da seqüência supercrescente (chave secreta) a partir da chave pública e dos parâmetros "trapdoor".

O algoritmo proposto por Shamir analisa a chave pública $a=(a_1,a_2,\ldots,a_n)$ a fim de determinar um par "trapdoor" de números naturais w e M tal que $(w.a_i \pmod M)_{i=1,n}$ seja uma seqüência supercrescente e a soma de seus elementos seja menor do que M. O conhecimento de um par qualquer de números com essas propriedades torna possível resolver todos os problemas mochila associados à seqüência $(a_1,a_2,\ldots,a_n)$, em tempo linear. Como os elementos a_i foram obtidos a partir de uma seqüência supercrescente por uma multiplicação modular, pelo menos um par "trapdoor" existe. O algoritmo determina algum par "trapdoor", mas não é garantido encontrar o módulo e o multiplicador (par original) utilizados na construção dos elementos a_i.

Na construção de Merkle-Hellman, os elementos da seqüência supercrescente original têm tamanhos conhecidos (mas valores desconhecidos!). Seja d a constante de proporcionalidade, com $1 < d < \infty$, então os elementos da seqüência supercrescentes podem ser escritos como:

Elemento	Tamanho(bits)	Valor
a'_1	dn-n	$< 2^{dn-n}$
a'_2	dn-n+1	$< 2^{dn-n+1}$
⋮	⋮	⋮
a'_i	dn-n+i-1	$< 2^{dn-n+i-1}$
⋮	⋮	⋮
a'_n	dn-1	$< 2^{dn-1}$

E o valor do módulo M será:

$$M \geq 2^{dn-n} + 2^{dn-n+1} + \ldots + 2^{dn-1} > \sum_{i=1}^{n} a'_i$$

$$M \cong 2 \cdot 2^{dn-1} \quad \therefore \quad M \cong 2^{dn}$$

$$2^{dn-1} < M < 2^{dn} \qquad \text{(III-6)}$$

Após a multiplicação modular, todos os números tornam-se , aproximadamnete, de tamanho dn bits.

$$a_i \rightarrow \text{dn bits} \quad \therefore \quad a_i < 2^{dn} \qquad \text{(III-7)}$$

O tamanho de M e, portanto, o tamanho de cada elemento a_i , cresce linearmente com n.

Os elementos a_i podem ser publicados em uma ordem permutada (isto é, a_1 não necessariamente corresponde ao menor elemento da seqüência supercrescente), mas ainda neste caso o algoritmo de Shamir permanece polinomial em n, mesmo se a permutação for desconhecida.

O algoritmo de Shamir é dividido em duas partes:

1ª Parte : Utiliza o algoritmo de Programação Inteira de Lenstra [48] para determinar um número racional α , $0 < \alpha \leq 1$, tal que a condição necessária para w e M formarem um par "trapdoor" é que a razão V=w/M pertença ao intervalo $[\alpha , \alpha + \varepsilon]$ para um certo ε pequeno.

2ª Parte : Utiliza o fato de que w/M é aproximadamente conhecido para proceder a uma análise mais apurada e dividir o intervalo $[\alpha , \alpha + \varepsilon]$ em subintervalos menores (ℓ_i , r_i). São determinados, no máximo, n^2 subintervalos (ℓ_i , r_i) em $[\alpha , \alpha + \varepsilon]$, tais que w/M pertença ao subintervalo (ℓ_i , r_i) é condição suficiente para w e M formarem um par "trapdoor". Supondo que algum par existe, então pelo menos um dos subintervalos tem que ser não-vazio. Empregando o algoritmo de aproximações diofantinas rápidas de Cassels [49], podem-se determinar os menores valores para w e M cuja razão esteja no subintervalo (ℓ_i , r_i).

Uma análise mais pormenorizada do algoritmo é apresentada a seguir.

Seja M_0 o módulo (desconhecido), de tamanho dn bits, usado na construção da seqüência $(a_i)_{i=1,n}$. O primeiro passo do algoritmo é generalizar a definição de um par "trapdoor" para considerar valores arbitrários positivos de w. O gráfico da função $w.a_i \pmod{M_0}$ para valores reais do multiplicador w , sendo $0 \leq w < M_0$, tem a forma de dente-de-serra:

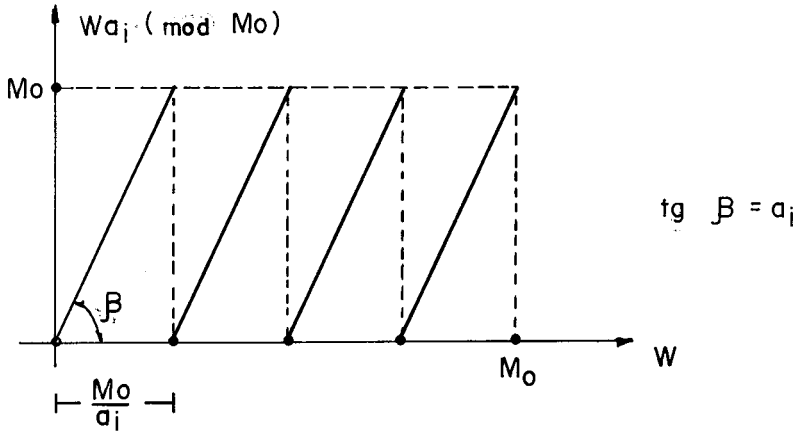


FIGURA III - 2 : REPRESENTAÇÃO GRÁFICA DA CURVA CORRESPONDENTE AO ELEMENTO a_i

O coeficiente angular da curva é a_i (exceto nos pontos de descontinuidade), o número de mínimos da função é a_i, e a distância entre dois mínimos sucessivos é M_0/a_i (que se supõe ser ligeiramente maior que 1, para efeito de simplificação).

Seja considerada a curva associada ao elemento a_1 (que corresponde, por hipótese, ao menor elemento da seqüência supercrescente). O multiplicador w_0 tem a propriedade de que $a_1' = w_0.a_1 \pmod{M_0}$ é, por construção, no máximo igual a 2^{dn-n}. Como a inclinação da curva é a_1 , a distância horizontal entre w_0 e o mínimo da curva a_1 mais próximo à sua esquerda não pode exceder $2^{dn-n}/a_1 \cong 2^{-n}$, como mostrado abaixo :

$$a_1' = w_0 \cdot a_1 \pmod{M_0} < 2^{dn-n}$$

$$a_1' = w_0\, a_1 - k\, M_0$$

$$\frac{a_1'}{a_1} = w_0 - k.\frac{M_0}{a_1}$$

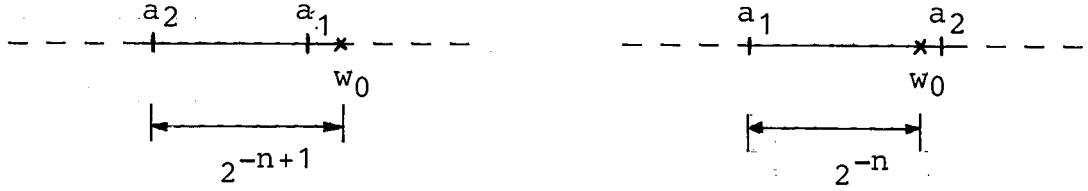
Δ : distância entre w_0 e o mínimo mais próximo à sua esquerda (porque $w_0 > k.\ M_0/a_1$)

$$\Delta \cong \frac{a_1'}{a_1} < \frac{2^{dn-n}}{2^{dn}} < 2^{-n}$$

Assim, o valor w_0 desconhecido deve estar muito próximo de algum mínimo da curva dente-de-serra a_1 . Infelizmente , mesmo impondo a restrição de w ser inteiro, existem muitos valores possíveis para w_0 e não podem ser testados um a um.

Uma análise similar mostra que w_0 deve também estar a uma distância de $2^{dn-n+1}/a_2 \cong 2^{-n+1}$ do mínimo mais próximo da curva a_2 à esquerda (esta curva corresponde, por hipótese, ao segundo elemento da seqüência supercrescente).

Desta forma, os dois mínimos das curvas a_1 e a_2 devem estar muito próximos um do outro. Dependendo da localização exata de w_0, o mínimo da curva a_2 pode estar até 2^{-n+1} à esquerda ou até 2^{-n} à direita do mínimo de a_1 :



Logo, a_1 e a_2 estão muito próximos um do outro. A condição de proximidade reduz extremamente o número de possibilidades de localização de w_0 mas, em muitos casos, ainda não o caracteriza unicamente.

Pode-se proceder de modo similar e superpor mais curvas no mesmo diagrama. O fato de que w_0 está próximo a um mínimo em cada curva, implica que todos esses mínimos estão próximos um do outro e, assim, o problema de determinar w_0 pode ser substituído pelo problema equivalente de determinar os pontos de acumulação

dos mínimos de várias curvas.

SHAMIR [27] mostrou que, superpondo quatro curvas, a probabilidade de ocorrer ponto de acumulação dos mínimos dessas curvas é muito pequena e, como pela construção dos elementos a_i existe w_0, garante que o ponto de acumulação é único no intervalo $0 \leq w < M_0$. Assim sendo, para determinar w_0 basta encontrar o ponto de acumulação para as quatro curvas superpostas.

Dois problemas ainda permanecem:

1- Como manipular M_0, cujo valor é desconhecido?

2- Como determinar o ponto de acumulação de quatro curvas superpostas?

A observação chave é que a localização do ponto de acumulação no diagrama depende da inclinação das curvas e não dos seus tamanhos. Dividindo-se ambas as coordenadas por M_0 , obtém-se a curva dente-de-serra da função $V.a_i \pmod 1$, $0 \leq V < 1$, que independe de M_0 :

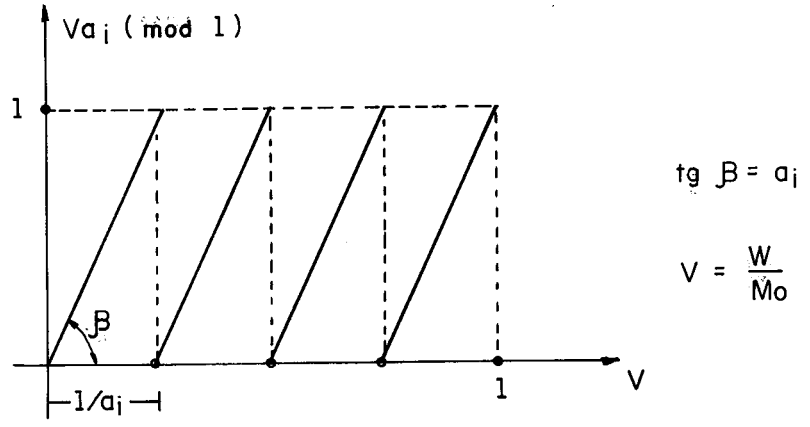


FIGURA III-3: REPRESENTAÇÃO GRÁFICA DA CURVA NORMALIZADA CORRESPONDENTE DO ELEMENTO a_i.

No novo sistema de coordenadas, a inclinação da curva permanece igual a a_i, o número de mínimos permanece a_i, mas a distância entre dois mínimos sucessivos é reduzida para $1/a_i$. O parâmetro original w_0 é substituído por um novo parâmetro $V_0 = w_0/M_0$, e a distância entre este parâmetro e o mínimo mais próximo da curva a_i é reduzido por um fator de aproximadamente 2^{dn} $(= M_0)$, isto é, de 2^{-n+i-1} para $2^{-dn-n+i-1}$.

O problema de localizar os pontos de acumulação dos mínimos das curvas no novo sistema de coordenadas pode ser descrito por inequações lineares com quatro incógnitas. Sem perda de generalidade, pode-se supor que a_1, a_2, a_3 e a_4 correspondem aos quatro menores elementos da seqüência supercrescente e, ainda, que o mínimo da curva a_1 é o mais próximo do ponto $V_0 = w_0/M_0$ (se assim não fosse, bastaria fazer uma permutação dos elementos a_i , i=1,n).

Para que o p-ésimo mínimo da curva a_1, o q-ésimo mínimo da curva a_2, o r-ésimo mínimo da curva a_3 e o s-ésimo mínimo da curva a_4 estejam suficientemente próximos um do outro é preciso que sejam satisfeitas as condições:

$$\begin{cases} p,\ q,\ r,\ s \ \text{inteiros} \\ 0 \le p/a_1 - q/a_2 \le 2^{-dn-n+1} \\ 0 \le p/a_1 - r/a_3 \le 2^{-dn-n+2} \\ 0 \le p/a_1 - s/a_4 \le 2^{-dn-n+3} \\ 1 \le p \le a_1 - 1 \\ 1 \le q \le a_2 - 1 \\ 1 \le r \le a_3 - 1 \\ 1 \le s \le a_4 - 1 \end{cases} \qquad \text{(III-8)}$$

Multiplicando-se as inequações pelos seus denominadores obtém-se o sistema equivalente:

$$\begin{cases} p,\ q,\ r,\ s \ \text{inteiros} \\ 0 \le p.a_2 - q.a_1 \le a_1.a_2.2^{-dn-n+1} \\ 0 \le p.a_3 - r.a_1 \le a_1.a_3.2^{-dn-n+2} \\ 0 \le p.a_4 - s.a_1 \le a_1.a_4.2^{-dn-n+3} \\ 1 \le p \le a_1 - 1 \\ 1 \le q \le a_2 - 1 \\ 1 \le r \le a_3 - 1 \\ 1 \le s \le a_4 - 1 \end{cases} \qquad \text{(III-9)}$$

onde p, q, r, s são as incógnitas e todos os demais valores são conhecidos. Todos os coeficientes de p, q, r e s são inteiros com não mais que dn bits.

Utilizando-se o algoritmo de programação inteira de LENSTRA [48], que é polinomial no tamanho dos coeficientes para um número fixo de incógnitas, pode-se determinar o (quase único) ponto de acumulação dos quatro mínimos das curvas em tempo polinomial. Este algoritmo é, também , um procedimento de decisão, que informa se um certo sistema de inequações lineares possui soluções inteiras.

Uma vez conhecido o valor de p, torna-se fácil determinar o intervalo $[\ \alpha,\ \alpha+\varepsilon\ ]$ (onde $\alpha = p/a_1$ e $\varepsilon \leq 1/a_1$) de valores de V no qual todas as n curvas correspondentes aos elementos $a_1, a_2, \ldots, a_n$ não apresentam ponto de descontinuidade e o valor dessas curvas é menor que 1.

Um diagrama típico de superposição das curvas, com a vizinhança de w_0/M_0 aumentada, é :

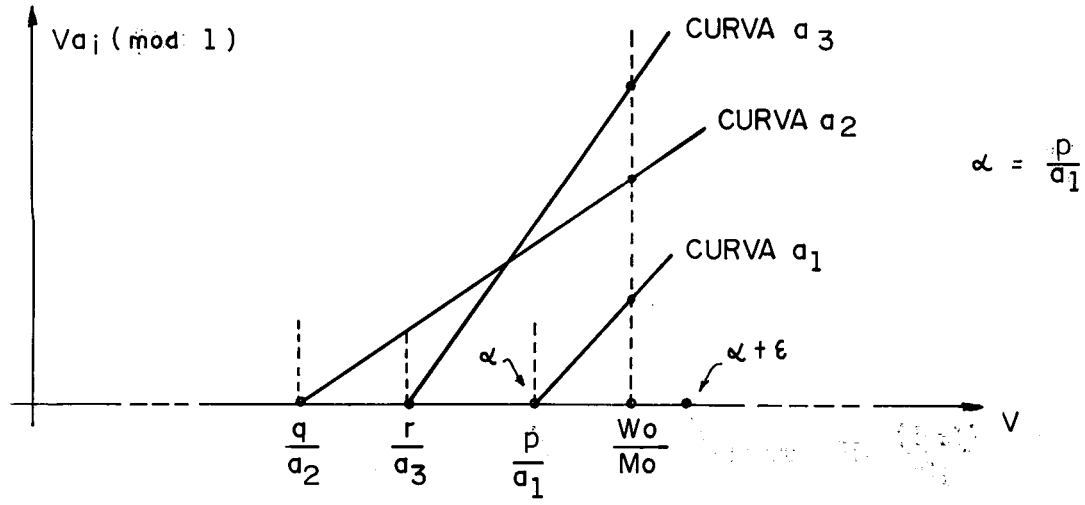


FIGURA III - 4: LOCALIZAÇÃO DA RAZÃO Wo / Mo

Qualquer par de números w_0 e M_0 tais que w_0/M_0 pertença ao intervalo $[\ \alpha,\ \alpha+\varepsilon\ ]$ fornece valores para as n curvas adequadamente limitados, após multiplicação modular, mas esses valores não necessariamente formam uma seqüência supercrescente e, desta forma, não conduzem a uma mochila facilmente solúvel.

A segunda parte do algoritmo descarta do intervalo $[\alpha, \alpha+\varepsilon]$ todos os subintervalos nos quais a seqüência transformada (valores no eixo vertical) não é supercrescente, ou a soma de seus elementos é maior que 1 (um). Os subintervalos remanescentes possuem a propriedade de que todo racional a eles pertencente corresponde a um par "trapdoor". Como w_0/M_0 não pode ser descartado por este processo, então algum subintervalo não-vazio deve permanecer. Portanto, a segunda parte do algoritmo extrai do intervalo $[\alpha, \alpha+\varepsilon]$ aqueles subintervalos (ℓ_i, r_i) nos quais é garantido que a seqüência transformada é supercrescente.

Uma vez que o intervalo $[\alpha, \alpha+\varepsilon]$ não contém pontos de descontinuidade, as n curvas dente-de-serra superpostas parecem como n segmentos de reta neste intervalo. Estes segmentos podem se interceptar dois-a-dois em, no máximo, $O(n^2)$ pontos. Determinando e ordenando esses pontos, pode-se subdividir o intervalo $[\alpha, \alpha+\varepsilon]$ em $O(n^2)$ subintervalos com uma ordem vertical bem definida entre as curvas em cada subintervalo. Quando esta ordem é conhecida, as condições para uma seqüência ser supercrescente podem ser expressas pelas desigualdades lineares:

$$\begin{cases} V \cdot a_{\P(i)} - C_{\P(i)} > \sum_{\P(j)<\P(i)} (V \cdot a_{\P(j)} - C_{\P(j)}) \\ \sum_{i=1}^{n} (V \cdot a_i - C_i) < 1 \qquad i,j = 1,\ldots,n \end{cases} \qquad \text{(III-10)}$$

onde: $\P$ - é a permutação dos índices, especificada pela ordenação vertical no subintervalo;

C_i - é o número de mínimos da curva a_i entre 0 (origem) e o ponto de acumulação;

V - é a incógnita a ser determinada.

A solução para cada conjunto de inequações é um (possivelmente vazio) subintervalo (ℓ_i, r_i) no qual as condições de supercrescimento e de tamanho são satisfeitas. Pelo menos um desses subintervalos deve ser não-vazio, e os menores números naturais w e M tais que $V = w/M$ pertença a esse subintervalo podem ser determinados em tempo polinomial.

Depois de encontrados os valores w e M (não necessariamente os valores originais w_0 e M_0), a criptoanálise de textos cifrados com a chave $a=(a_1,a_2,\ldots,a_n)$ torna-se trivial.

III.2.2.2.2.3 - TÉCNICA DE BRICKELL-SIMMONS

Como decorrência de uma análise do método de ataque descrito em [27], e apresentado no item anterior, BRICKELL e SIMMONS [29] propuseram uma técnica de criptoanálise que se constitui numa versão melhorada do algoritmo desenvolvido por SHAMIR [27].

A técnica de Shamir baseia-se na determinação de um valor $V_0 = w_0/M_0$, que é equivalente ao problema de determinar o ponto de acumulação dos mínimos de quatro curvas superpostas (uma vez que a distância entre V_0 e esses mínimos é extremamente pequena). Este problema pode ser caracterizado pelas seguintes inequações lineares :

$$\begin{cases} 0 \leq C_1/a_1 - C_2/a_2 \leq 2^{-dn-n+1} \\ 0 \leq C_1/a_1 - C_3/a_3 \leq 2^{-dn-n+2} \\ 0 \leq C_1/a_1 - C_4/a_4 \leq 2^{-dn-n+3} \end{cases} \qquad \text{(III-11)}$$

onde $C_i \geq 0$ é o número de mínimos da curva a_i entre 0(zero) e o valor V_0 onde as quatro curvas satisfazem simultaneamente a condição $a_i' < 2^{-dn+i-1}$ (valor, no eixo vertical, da curva correspondente ao elemento a_i).

O algoritmo de Shamir baseia-se na expectativa de que, se para alguma escolha de quatro elementos da seqüência $(a_i)_{i=1,n}$ os mínimos das curvas correspondentes se acumulam muito próximos um do outro, isto é, se existem quatro inteiros C_i satisfazendo o sistema (III-11), então este (quase certamente único) ponto é muito próximo de $V_0 = w_0/M_0$.

A distância entre V_0 e o mínimo da curva a_i mais próximo a sua esquerda é:

$$\frac{a'_i}{a_i} \cdot \frac{1}{M_0} = V_0 - \frac{C_i}{a_i} \qquad \text{(III-12)}$$

[Lembrar que $a'_i = a_i.w_0 - C_i.M_0$ e que $V_0 \doteq w_0/M_0$] ,

e assim o mínimo mais próximo da curva a_i está localizado em:

$$\frac{C_i}{a_i} = V_0 - \frac{a'_i}{a_i} \cdot \frac{1}{M_0} \qquad \text{(III-13)}$$

Substituindo esses valores no sistema (III-11) e multiplicando todos os termos por M_0, obtém-se o sistema de inequações equivalente:

$$\begin{cases} 0 \leq a'_2/a_2 - a'_1/a_1 \leq M_0.2^{-dn-n+1} \\ 0 \leq a'_3/a_3 - a'_1/a_1 \leq M_0.2^{-dn-n+2} \\ 0 \leq a'_4/a_4 - a'_1/a_1 \leq M_0.2^{-dn-n+3} \end{cases} \qquad \text{(III-14)}$$

onde $(a'_i)_{i=1,n}$ é a seqüência supercrescente e $(a_i)_{i=1,n}$ é a chave pública.

O ponto essencial, no qual o algoritmo de Shamir se apóia, é que os valores das razões a'_i/a_i para os menores elementos da mochila de Merkle-Hellman são extremamente pequenos, isto é, $a'_1/a_1 \cong 2^{-n}$, $a'_2/a_2 \cong 2^{-n+1}$, etc... Consequentemente, com uma probabilidade muito grande, para mochilas "trapdoor" aleatoriamente construídas, a diferença das menores razões são correspondentemente pequenas. A forma do sistema (III-14) e as observações acima sugerem um meio para o usuário do Criptossistema Merkle-Hellman fugir ao ataque de Shamir. Se o usuário puder forçar que um dos elementos a'_2, a'_3 ou a'_4 seja representado

por um elemento a_i muito pequeno, então a inclinação da curva a_i correspondente será menor que a esperada e o mínimo mais próximo desta curva estará mais distante à esquerda de V_0 que o esperado, o que pode implicar que uma ou mais inequações do sistema (III-14) não tenha solução.

Portanto, não é, necessariamente, verdade que, na vizinhança de um ponto onde as quatro curvas são simultaneamente muito pequenas, todos os mínimos dessas curvas estão também muito próximos um do outro.

A técnica de Brickell-Simmons é similar ao ataque criptoanalítico de Shamir, com pequenas modificações para determinar a localização de $V_0 = w_0/M_0$.

Todos os aspectos desse algoritmo proposto são idênticos ao método de Shamir : o sistema de inequações possui a mesma forma, o procedimento para determinar os subintervalos é o mesmo, são realizados os mesmos testes para as condições de supercrescimento, unicidade e de tamanho. Apenas o modo de localizar as regiões nas quais pode estar a solução é diferente.

A diferença básica entre os dois métodos é que SHAMIR [27] tenta localizar V_0 procedendo a uma busca no eixo horizontal para encontrar o ponto de acumulação dos mínimos das curvas superpostas, enquanto BRICKELL e SIMMONS [29] executam a busca no eixo vertical, para determinar o ponto de acumulação dos valores da função " $V.a_i \pmod 1$ ".

Em ambos os casos o parâmetro essencial do algoritmo é a razão entre os elementos correspondentes das seqüências fácil e difícil, a'_i/a_i , respectivamente. Empregando um esforço inicial de computação, é possível fazer com que esta razão difira grandemente do valor esperado e desta forma acarrete o fracasso do sistema de inequações de Shamir sem, no entanto, afetar o algoritmo de Brickell-Simmons, isto é, o usuário do sistema de chave pública de Merkle-Hellman pode gerar uma mochila difícil que é imune ao algoritmo criptoanalítico proposto por Shamir , mas não ao de Brickell-Simmons.

Ao final da execução do algoritmo de Brickell-Simmons são obtidos os valores para um par "trapdoor" w,M (não necessariamente o par original).Com esses valores, e conhecida a chave pública, obtém-se uma chave supercrescente, que torna trivial a decifração de qualquer criptograma .

III.2.2.2.3 - ANÁLISE CRÍTICA

Pelas técnicas apresentadas anteriormente, observa-se que a propriedade de supercrescimento da seqüência original empregada no criptossistema de Merkle-Hellman para fornecer a chave pública, e também a linearidade das operações utilizadas, constituem uma fraqueza criptográfica, permitindo ao criptoanalista "quebrar" o sistema para quase todas as escolhas de representação modular.

As três formulações descritas para ataque à informação "trapdoor", EIER-LAGGER [25], SHAMIR [27] e BRICKELL-SIMMONS [29], se aplicam ao caso de mochila de iteração simples e para seqüência original supercrescente. Uma propriedade importante dessas três técnicas é que analisam diretamente a chave pública, em vez dos valores dos criptogramas, para recuperar a informação secreta. Essas técnicas se baseiam na determinação da razão $V = w/M$, da seguinte forma:

- Eier e Lagger utilizam o conceito de M-dominância, considerando uma função resultante da soma de todas as funções elementares;
- Shamir utiliza o conceito de ponto de acumulação, no eixo horizontal, dos mínimos das curvas correspondentes aos elementos a_i superpostas, bastando considerar apenas quatro curvas; e
- Brickell e Simmons também empregam o conceito de ponto de acumulação e consideram apenas quatro curvas superpostas, mas a análise focaliza a distribuição dos valores das curvas no eixo vertical.

A técnica de Eier-Lagger para determinar a informação "trapdoor" utiliza todas as curvas normalizadas, correspondentes aos elementos da mochila, para proceder à criptoanálise. O algoritmo determina a região provável de localização das soluções $V = w/M$, analisando os intervalos em que é satisfeita a propriedade de tamanho (isto é, onde a soma das curvas elementares é menor que 1), sem considerar, explicitamente, a propriedade de supercrescimento. O que pode ser feito é uma verificação posterior à determinação dos parâmetros w e M para ver se estes geram uma seqüência supercrescente.

A técnica criptoanalítica de Shamir é mais eleborada, e a sua primeira grande inovação foi a de analisar a localização aproximada da razão $V_0 = w_0/M_0$ determinando o seu valor pelo ponto de acumulação dos mínimos de quatro curvas superpostas. A segunda foi a observação de que o problema assim resultante pode ser formulado como um problema de programação linear inteira, podendo ser resolvido, em tempo polinomial, empregando-se o algoritmo de LENSTRA [48]. Determinado um valor V_0 , são então consideradas as n curvas para testar as condições de supercrescimento e tamanho, a fim de obter os menores valores w_0 e M_0 que satisfazem a essas propriedades (a seqüência transformada tem que ser supercrescente e a soma dos seus elementos tem que ser menor do que M_0).

Para informações "trapdoor" aleatoriamente escolhidas (w_0,M_0) , $M_0 > \sum_{i=1}^{n} a_i$, o algoritmo criptoanalítico de Shamir consegue quebrar o criptossistema de Merkle-Hellman de iteração simples, em tempo polinomial, com probabilidade de sucesso tendendo a 1 (um) exponencialmente com o aumento do tamanho da mochila. Uma condição importante para o sucesso do ataque de Shamir é que a relação entre os termos extremos da mochila original seja grande (o que ocorre numa seqüência supercrescente). Portanto, para os casos em que esta relação é diferente da esperada (ou seja, o seu valor é pequeno), o ataque de Shamir pode se tornar ineficiente. Neste caso pode-se tentar aplicar a técnica de Brickell-Simmons, como descrito em [29].

A técnica de Brickell-Simmons é similar à de Shamir e, por isso, não necessita maiores comentários. Apenas deve ser ressaltado que o fato da busca da solução ser processada no eixo vertical (ponto de acumulação dos valores das curvas a_i e não de seus mínimos) garante melhor desempenho do algoritmo , podendo ser usado em alguns casos em que o de Shamir fracassa. A região inicial para verificação da solução é aquela em que ocorre o mínimo de uma das curvas, mas as propriedades de supercrescimento e tamanho têm que ser satisfeitas para todas as n curvas.

As técnicas de ataque à informação "trapdoor" mostraram que quase todos os criptossistemas Merkle-Hellman de iteração simples, nos quais os elementos da chave pública são obtidos a partir de seqüências supercrescentes por multiplicação modular, podem ser quebrados em tempo polinomial e, portanto , são totalmente inseguros. Nenhuma das técnicas aqui apresentadas até agora se aplica ao caso de mochila de múltipla iteração.

III.2.2.3 - MOCHILA DE ITERAÇÃO MÚLTIPLA

III.2.2.3.1 - INTRODUÇÃO

Em fins de 1982 ADLEMAN [33] publicou um importante trabalho na área de criptoanálise, apresentando um esboço de ataque ao criptossistema Merkle-Hellman de iteração múltipla , até então um problema em aberto. Aquele autor foi o primeiro a sugerir o uso do algoritmo de Lenstra, Lenstra Jr e Lovász (L^3) para redução de base de reticulado [50] em ataques aos criptossistemas mochila, sendo agora este algoritmo uma das mais úteis ferramentas usadas em técnicas de ataque criptoanalítico. Em 1983 ADLEMAN [34] propôs, então, uma técnica mais elaborada de ataque ao método de iteração múltipla do esquema de Merkle-Hellman, onde o problema criptográfico é tratado como um problema matricial (utilizando o algoritmo L^3), e não como um problema de programação linear, como considerado por SHAMIR [27] e por BRICKELL e SIMMONS [29].

A idéia básica da técnica de Adleman é a recuperação da informação "trapdoor", isto é, dos pares (w_j, M_j) utilizados nas iterações sucessivas da mochila, para então decifrar todas as mensagens.

Vale ressaltar que as técnicas de ataque a mochilas de iteração simples se propõem a determinar algum par "trapdoor" w,M (mas não necessariamente é garantido encontrar o par original) tal que sejam satisfeitas as condições de supercrescimento e tamanho para a seqüência transformada. No entanto, no caso de mochilas de iteração múltipla, ao contrário do que ocorre nos ataques a mochilas de iteração simples, somente os valores originais w_j e M_j , $j=1,..,z$, utilizados nas z iterações, permitem ao criptoanalista executar a multiplicação modular inversa apropriada e atacar as iterações intermediárias uma-a-uma.

Apesar dos esforços de Adleman, ainda não foi possível apresentar uma prova rigorosa de que seu algoritmo funcione, e, por isso, serão apresentadas as características da técnica de ataque e uma análise de seu desempenho em presença de hipóteses razoáveis.

III.2.2.3.2 - CARACTERÍSTICAS DA TÉCNICA DE ADLEMAN

Para segurança do criptossistema de Merkle-Hellman é importante que o problema de se obter a chave secreta a partir da chave pública seja intratável. No entanto, com os ataques criptoanalíticos que se baseiam na determinação da informação "trapdoor", uma vez determinados os parâmetros w e M, e conhecendo-se a chave pública, torna-se trivial a obtenção de uma chave equivalente à chave secreta, bastando aplicar a transformação modular inversa.

Nos criptossistemas mochila de iteração múltipla os pares de chaves são gerados de acordo com o procedimento a seguir:

Passo 0 : Definir inteiros positivos n (tamanho da mochila) e z (número de iterações desejadas), e gerar a seqüência $a_0 = (a_{0,1} , a_{0,2} , \ldots , a_{0,n})$ tal que:

$$a_{0,i} > \sum_{j=1}^{i-1} a_{0,j} \qquad i = 2,3,\ldots,n \quad \text{e} \quad a_{0,1} > 0$$

Passo 1 : Gerar inteiros positivos w_1 e m_1 tais que:

a) $(w_1 , m_1) = 1$

b) $m_1 > \sum_{i=1}^{n} a_{0,i}$

Calcular:

$$a_{1,i} \equiv w_1 \cdot a_{0,i} \pmod{m_1} \quad , \; i = 1,\ldots,n$$

⋮

Passo z : Gerar inteiros positivos w_z e m_z tais que :

a) $(w_z , m_z) = 1$

b) $m_z > \sum_{i=1}^{n} a_{z-1,i}$

Calcular:

$$a_{z,i} \equiv w_z \cdot a_{z-1,i} \pmod{m_z} \quad , \; i = 1,\ldots,n$$

Passo z+1 : Definir uma permutação ¶ para os elementos da seqüência $(a_{z,i})_{i=1,n}$ obtendo-se a seqüência permutada $(a_i)_{i=1,n}$, que é tornada pública.

A chave pública é:

$a = (a_1, a_2, \ldots, a_n)$

A chave secreta é:

$a_0 = (a_{0,1}, a_{0,2}, \ldots, a_{0,n})$

E os parâmetros secretos são:

$[(w_1,m_1), (w_2,m_2), \ldots, (w_z,m_z)]$

A idéia básica da técnica criptoanalítica de ADLEMAN [34] é determinar a chave secreta, a partir do conhecimento da chave pública, por um processo iterativo, obtendo-se inicialmente $w=w_z$ e $m=m_z$ e repetindo-se o processo. Na realidade, como são utilizadas transformações modulares inversas no processo de criptoanálise, serão determinados $u = w^{-1} \pmod m$ e m.

Por construção, existem números naturais $k_1, k_2, \ldots, k_n$ tais que (a menos da permutação dos elementos da chave pública):

$$u.a_i - k_i.m = a_{z-1,i} \qquad i=1,\ldots,n \qquad \text{(III-15)}$$

onde os elementos a_i são conhecidos, pois constituem a chave pública, e os elementos $a_{z-1,i}$ formam a seqüência imediatamente anterior à obtenção da chave pública no processo iterativo (a partir de agora serão denominados de b_i).

Para começar o ataque, o criptoanalista escolhe, aleatoriamente, um subconjunto T de d elementos a_i da chave pública e define:

$$S = \{ i \mid a_i \in T \}$$

Pode-se, então, escrever o seguinte sistema de equações:

$$U.a_i - K_i.M = B_i \quad , \quad i \in S \qquad \text{(III-16)}$$

onde as letras maiúsculas caracterizam as incógnitas e as minúsculas os valores conhecidos.

Este sistema apresenta as seguintes propriedades:

i) O sistema é subdeterminado, possuindo uma infinidade de soluções.

ii) Dentre as soluções [U, M, $\{K_i\}_{i\in S}$, $\{B_i\}_{i\in S}$] está a solução desejada [u, m, $\{k_i\}_{i\in S}$, $\{b_i\}_{i\in S}$].

iii) Existem muitas soluções indesejadas, isto é, que não satisfazem a todas as equações do problema completo (quando considerando todos os elementos da chave pública), apenas servem para o problema reduzido (considerando o conjunto S)

iv) O sistema é não-linear (devido aos termos $K_i.M$) e não se conhece um algoritmo em tempo polinomial para resolvê-lo.

Para ser possível solucionar o sistema (III-16) Adleman sugeriu a sua simplificação (com a remoção de algumas incógnitas) e também utilizou algumas considerações partindo das características de construção do sitema mochila de Merkle-Hellman, como mostrado a seguir.

No criptossistema mochila de Merkle-Hellman tem-se, por construção, que $M > b_i$, $i=1,2,\ldots,n$. Portanto existe um valor máximo "e" , tal que $M/2^e > b_i$, $i \in S$. (Supõe-se que este valor é conhecido pelo criptoanalista). Isso permite escrever:

$$0 < U.a_i - K_i.M \leq M/2^e \quad , \quad i \in S \qquad \text{(III-17)}$$

O sistema (III-17) apresenta uma infinidade de soluções e, dentre estas, pode-se garantir que existirá ainda uma solução quando um inteiro "f" suficientemente grande (bem mai-

or que m) for considerado para substituir M. Pode-se escrever então:

$$0 < U.a_i - K_i.f \leq f/2^e \quad , \quad i \in S \qquad \text{(III-18)}$$

O sistema (III-18) apresenta algumas propriedades que devem ser mencionadas:

i) O sistema é linear, pois são conhecidos os elementos a_i , e os valores "e" e "f", e portanto pode-se aplicar o algoritmo L^3 de Lenstra, Lenstra Jr e Lovász para determinar a solução.

ii) Dentre as soluções do sistema (III-18) existe pelo menos uma da forma $[\ U, \{k_i\}_{i \in S}\ ]$ onde os elementos k_i são exatamente os mesmos para a "solução desejada" do sistema (III-17).

iii) Para $U = 1,2,\ldots \lfloor f/2^e.a \rfloor$, onde $a = \max \{ a_i \}_{i \in S}$, existem soluções para o sistema (III-18) da forma $[\ U, \{0\}_{i \in S}\ ]$.

iv) Para um valor suficientemente grande "d", existe uma grande probabilidade de o sistema (III-18) não admitir outras soluções que aquelas indicadas nos itens anteriores.

Para resolver o sistema (III-18) é utilizado o algoritmo de redução de base de reticulado de LENSTRA, LENSTRA Jr. e LOVÁSZ [50], que possui as seguintes propriedades:

1ª - Para vetores $V_1, V_2, \ldots, V_n$ em $\mathbb{R}^n$ do reticulado L , gera vetores $V_1^*, V_2^*, \ldots, V_n^*$ em $\mathbb{R}^n$ e inteiros $q_{i,j}$, $1 \leq i,j \leq n$ tais que:

$$V_i^* = q_{i,1}.V_1 + q_{i,2}.V_2 + \ldots + q_{i,n}.V_n \qquad i=1,2,\ldots,n$$

$$| V_i^* | \leq 1,34^{(n-1)/2}. | \lambda_i | \qquad i=1,2,\ldots,n$$

onde $| V |$ é a norma Euclideana de V e λ_i é o i-ésimo mínimo sucessivo no reticulado L (isto é, λ_i é o vetor

não nulo de menor norma Euclideana em L que não é uma combinação linear de λ_1 , λ_2 ,..., λ_{i-1}).

2ª - O algoritmo é processado em tempo polinomial.

Seja o reticulado L gerado pelos seguintes vetores:

$$V_1 = (\hat{a}_1, \hat{a}_2, \ldots, \hat{a}_d, 0)$$
$$V_2 = (f , 0 , \ldots, 0 , 0)$$
$$V_3 = (0 , f , \ldots, 0 , 0)$$
$$\vdots$$
$$V_{d+1} = (0 , 0 , \ldots, f , 0)$$

onde $\hat{a}_j$ é o j-ésimo elemento em T.

O reticulado L contém os seguintes vetores:

$$W_1 = (\hat{a}_1, \hat{a}_2, \ldots, \hat{a}_d, 0) = 1.V_1 + 0.V_2 + \ldots + 0.V_{d+1}$$
$$W_2 = (2\hat{a}_1, 2\hat{a}_2, \ldots, 2\hat{a}_d, 0) = 2.V_1 + 0.V_2 + \ldots + 0.V_{d+1}$$
$$\vdots$$
$$W_{\lfloor f/2^e.a \rfloor} = (\lfloor f/2^e.a \rfloor \hat{a}_1, \ldots, \lfloor f/2^e.a \rfloor \hat{a}_d, 0) = \lfloor f/2^e.a \rfloor .V_1 + \ldots + 0.V_{d+1}$$

$$Y_0 = (g_{1,1}, g_{1,2}, \ldots, g_{1,d}, 0) = \hat{U}_0.V_1 + k_1.V_2 + \ldots + k_d.V_{d+1}$$
$$\vdots$$
$$Y_z = (g_{z,1}, g_{z,2}, \ldots, g_{z,d}, 0) = \hat{U}_z.V_1 + k_1.V_2 + \ldots + k_d.V_{d+1} .$$

para alguns inteiros $\hat{U}_z$ (de fato $\hat{U}_z = \hat{U}_0 + z$) e onde $| Y_0 | \leq \sqrt{d} . f/2^e$.

Como todos os vetores W_i são múltiplos de W_1, segue-se que, se o reticulado L não contiver nenhum outro vetor X tal que $|x| \leq \sqrt{d} \cdot f/2^e$, então $\lambda_2 = Y_0$.

Infelizmente o algoritmo de redução de base de reticulado não garante encontrar λ_2 (e, por conseguinte, os valores k_i desejados), mas é garantido apenas encontrar um vetor V_2^*, o qual não é muito grande :

$$|V_2^*| < 1{,}34^{d/2} \cdot |\lambda_2| \leq 1{,}34^{d/2} \cdot \sqrt{d} \cdot f/2^e$$

Se, no entanto, for garantido que L não contém nenhum vetor "excepcional" Y diferente dos vetores W_i e Y_i - tal que $|X| \leq 1{,}34^{d/2} \cdot \sqrt{d} \cdot f/2^e$ -, então o algoritmo de redução de base fornecerá um dos vetores U_i como sendo V_2^* e, portanto, podem ser obtidos os valores k_i desejados.

Deve ser lembrado que, aumentando-se o valor d, reduz-se a probabilidade de L conter um vetor "excepcional" mas, por outro lado, aumenta-se a imprecisão do algoritmo de redução de base. Um valor ótimo para d, segundo ADLEMAN [34], é tal que:

$$\left\{ \frac{2^e}{\sqrt{d} \cdot (1{,}34^{d/2})} \right\}^d > 2m \qquad \text{(III-19)}$$

ou, tomando-se logaritmos na base 2 vem :

$$e.d - d/2.\log d - d^2/2.\log(1{,}34) > \log(m) + 1 \qquad \text{(III-20)}$$

Resolvido o sistema (III-18), após a aplicação do algoritmo L^3, o valor U pode não corresponder ao valor correto desejado para esta variável (devido ao valor impreciso f utilizado para M), mas os valores k_i obtidos são corretos, isto é, são os mesmos que seriam obtidos caso tivesse sido usado o valor M correto.

Retornando-se ao ataque criptoanalítico, com os valores k_i determinados, pode-se eliminar a não-linearidade do sistema (III-17) substituindo-se os valores já conhecidos destas variáveis. Então, pode-se escrever:

$$0 < U.a_i - k_i.M \leq M/2^e \quad , \quad i \in S \qquad \text{(III-21)}$$

Segundo ADLEMAN [34], o sistema (III-21) possui as seguintes propriedades:

i) É linear e, portanto, existe um algoritmo em tempo polinomial para resolvê-lo.

ii) Dentre as soluções [U, M] está a solução desejada (u, m).

iii) Existem muitas soluções indesejadas.

É preciso distinguir (u, m) das outras soluções. O que caracteriza a solução (u, m) como especial é que:

$$u.a_i - k_i.m = b_i \qquad \text{(III-22)}$$

onde b_i é o resultado do passo anterior no processo de geração da chave pública. Desta forma, existem inteiros $\hat{e}$, $\hat{u}$, $\hat{m}$, $\hat{k}_i$ tais que:

$$\hat{u}.b_i - \hat{k}_i.\hat{m} = c_i \qquad \text{(III-23)}$$

e

$$\hat{u}.b_i - \hat{k}_i.\hat{m} \leq \hat{m}/2^{\hat{e}} \qquad \text{(III-24)}$$

Usando um procedimento similar àquele empregado para determinar os valores k_i , podem-se obter os valores $\hat{k}_i$, da seguinte forma:

$$0 < U.a_i - k_i.M \leq M/2^e \quad , \quad i \in S$$

$$0 < U.a_i - k_i.M - \hat{k}_i.f \leq f/2^e \quad , \quad i \in S \qquad \text{(III-25)}$$

onde $f > 2^{e}.b_i$, $i \in S$ e "d" satisfaz as expressões (III-19) e (III-20). Assim pode-se obter, para o problema do reticulado correspondente, o vetor V_3^* cuja representação, como uma combinação linear dos vetores de entrada, fornecerá os valores $\hat{k}_i$, $i \in S$.

Obtidos os valores $\hat{k}_i$, pode-se considerar, finalmente o sistema:

$$\begin{aligned} &0 < U.a_i - k_i.M \leq M/2^{e} \quad , \qquad i \in S \\ &0 < U.a_i - k_i.M - \hat{k}_i.\hat{M} \leq \hat{M}/2^{\hat{e}} \qquad i \in S \end{aligned} \tag{III-26}$$

Resolvendo o sistema (III-26), utilizando o algoritmo de redução de reticulado, obtém-se a solução [U, M, $\hat{M}$] , com a seguinte propriedade:

$$\frac{U}{(U,M)} = u \quad , \qquad \frac{M}{(U,M)} = m \tag{III-27}$$

Desta forma são recuperados os parâmetros "trapdoor" da multiplicação modular, usados no último passo do processo de obtenção da chave pública.

De posse dos valores u , m e conhecida a chave pública, utiliza-se a equação (III-15) para determinar os elementos $a_{z-1,i}$ (seqüência anterior, no processo de geração de chave, à chave pública) e, desta forma, obter uma mochila com z-1 iterações. A esta mochila pode ser aplicado, repetidamente, o processo de Adleman, obtendo-se para cada iteração j os valores u_j, m_j correspondentes. Ao final das z iterações obter-se-á uma seqüência supercrescente, caracterizando o fim do processo iterativo.

III.2.2.3.3 - ANÁLISE CRÍTICA

A técnica de ataque proposta por ADLEMAN [34] é um algoritmo, em tempo polinomial, para tentar quebrar o sistema de iteração múltipla de Merkle-Hellman.

Como já mencionado anteriormente, a propriedade de supercrescimento da seqüência original (chave de decifrar) empregada no criptossistema de Merkle-Hellman para gerar a chave pública, e também a linearidade das operações utilizadas, constitui em fraqueza criptográfica, que é explorada pelos criptoanalistas para quebrar o sistema Merkle - Hellman de iteração simples e de iteração múltipla.

O método de ataque descrito acima analisa apenas os elementos da chave pública (e das seqüências intermediárias, no processo iterativo) para determinar os parâmetros "trapdoor" utilizados nas transformações modulares do processo de geração da chave de cifrar, a partir da seqüência supercrescente.

A técnica de criptoanálise proposta por ADLEMAN [34], foi avaliada por BRICKELL, LAGARIAS e ODLYZKO [57], que mostraram que essa técnica muitas vezes não funciona, mesmo quando restrita a mochilas de iteração dupla.

O método de ataque de Adleman ao sistema mochila de iteração múltipla consiste em três etapas principais:

1ª - Usar o fato de que $m_z > \sum_{i=1}^{n} a_{z-1,i}$ para determinar $k_{z,1}$ pela aplicação do algoritmo L^3.

2ª - Usando $k_{z,i}$ determinado no passo anterior, e com uma outra aplicação do algoritmo L^3, determinar $k_{z-1,i}$.

3ª - Usando $k_{z,i}$ e $k_{z-1,i}$ determinados nos passos anteriores, aplicar o algoritmo L^3 para determinar m_z e w_z .

Uma vez que o 3º passo tenha sido completado com sucesso, pode-se facilmente descobrir os elementos $a_{z-1,i}$, e então obtém-se uma mochila com z-1 iterações, à qual poderá ser aplicada a mesma técnica descrita acima (se $z > 2$) ou então o ataque de Shamir (se $z=2$).

Os resultados da avaliação feita por Brickell, Lagarias e Odlyzko podem ser resumidos como a seguir:

- O 1º Passo do ataque de Adleman não obteve sucesso quando testado para o reticulado particular sugerido em [34]. Entretanto, uma simples modificação neste reticulado conduz a, pelo menos, um sucesso parcial.
- Testes empíricos indicaram que o reticulado modificado normalmente contém $z+1$ vetores pequenos (uma explicação heurística para isso é dada pelos argumentos apresentados por LAGARIAS [36]) e que o vetor desejado que fornece os $k_{z,i}$ é uma combinação linear desses $z+1$ vetores pequenos com coeficientes muito pequenos. Então, para valores pequenos de z , parece viável testar todos os possíveis candidatos para os $k_{z,i}$.
- O 3º Passo do ataque de Adleman não funcionou como sugerido. Entretanto, é possível descobrir m_z e w_z a partir do conhecimento de $k_{z,i}$ e $k_{z-1,i}$, muito mais facilmente sem o uso do algoritmo L^3.
- Apesar de existirem dificuldades com os passos 1º e 3º do ataque de Adleman, elas não são insuperáveis.No entanto, este parece não ser o caso de 2º Passo. Neste caso, o reticulado sugerido por Adleman, como também várias modificações nele tentadas, continha alguns vetores muito pequenos, muito menores que o vetor procurado. (Pode-se provar a existência desses vetores pequenos, e que estão relacionados com aproximações racionais pequenas para w_z^{-1} / m_z , onde $w_z . w_z^{-1} \equiv 1 (\mathrm{mod}\ m_z)$). Isso significa que o vetor desejado não pode ser distinguido dos muitos outros vetores de tamanho similar,e portanto o 2º Passo provavelmente não pode ser executo como descrito no artigo de ADLEMAN [34].

Pelo que foi mostrado anteriormente, conclui-se que o sucesso do método de ataque de Adleman está intimamente relacionado ao desempenho do algoritmo L^3. Como citado em [34], o próprio Adleman não se aprofundou muito na análise de seu método, e também não foi capaz de apresentar uma prova rigorosa de que o ataque seja eficaz.

Uma idéia a ser estudada é a possibilidade de "resolver" o sistema com um número de iterações menor que o utilizado no algoritmo de geração da chave pública.

III.2.3 - RECUPERAÇÃO DA MENSAGEM DIRETAMENTE

III.2.3.1 - CONSIDERAÇÕES

Os métodos de ataque descritos a seguir consistem na recuperação da mensagem diretamente, em vez de obter a chave secreta (informação "trapdoor") para depois, então, decifrar o criptograma (obter o texto claro).

Os ataques mostrados anteriormente são baseados na idéia de recuperar a informação "trapdoor" escondida nos elementos $\{ a_i : 1 \leq i \leq n \}$, isto é, o criptoanalista, manipulando apenas os inteiros $a_1, a_2, \ldots, a_n$ tenta encontrar a informação secreta que permitirá decifrar qualquer mensagem, ou seja, resolver qualquer problema mochila associado aos inteiros $a_1, a_2, \ldots, a_n$. Já para os métodos apresentados a seguir, a filosofia de ataque é bastante diferente, uma vez que a idéia básica é determinar diretamente uma solução viável $x = (x_1, x_2, \ldots, x_n)$ para o problema mochila, e não recuperar a informação "trapdoor".

As técnicas de criptoanálise que apresentam esta nova filosofia consideram, na sua formulação, basicamente, o conhecimento dos elementos da chave pública, dos criptogramas e das características de construção do criptossistema de chave pública de Merkle-Hellman.

A seguir são apresentados os métodos criptoanalíticos que recuperam a mensagem diretamente, os quais podem ser de ataque ao criptograma somente (método matricial e método gráfico), ataque por reduções sucessivas (utilizando transformações modulares) e ataque a mochilas de baixa densidade.

III.2.3.2 - ATAQUE AO CRIPTOGRAMA

III.2.3.2.1 - MÉTODO MATRICIAL

III.2.3.2.1.1 - CARACTERÍSTICAS GERAIS

MILLER [11] apresentou um ataque criptoanalítico, do tipo "criptograma conhecido", para ser efetuado contra o criptossistema mochila de chave pública.

A técnica se aplica quando uma mesma mensagem é cifrada com diferentes chaves e transmitida simultaneamente para os diversos usuários do sistema (o que caracteriza a utilização do criptossistema em situações de "broadcast").

No caso em que o número de usuários que deverão receber a mensagem é, pelo menos, igual ao número de elementos da chave criptográfica (isto é, a mensagem será transmitida , pelo menos, n vezes), a cifração do texto claro pode ser representada pela equação matricial :

$$S = A.x \qquad \text{(III-28)}$$

onde: $S = (S^{(1)}, S^{(2)}, \ldots, S^{(n)})^T$ é o vetor dos criptogramas, sendo cada elemento $S^{(k)}$ o criptograma efetivamente transmitido ao usuário k ;

$$A = \begin{bmatrix} a_1^{(1)} & a_2^{(1)} & \cdots & a_n^{(1)} \\ a_1^{(2)} & a_2^{(2)} & \cdots & a_n^{(2)} \\ \vdots & & & \\ a_1^{(n)} & a_2^{(n)} & \cdots & a_n^{(n)} \end{bmatrix}$$

é a matriz de chaves públicas, sendo cada linha $a^{(k)} = (a_1^{(k)}, a_2^{(k)}, \ldots, a_n^{(k)})$ a chave de cifrar do usuário k ;

$x = (x_1, x_2, \ldots, x_n)^T$ é o vetor binário que representa a mensagem a ser transmitida a todos os destinatários.

Usando a equação (III-28), e conhecidos os criptogramas dos diversos destinatários, torna-se fácil o problema de determinar o texto claro x, pois :

$$x = A^{-1} . S \qquad \text{(III-29)}$$

A matriz A possui, por construção, grande probabilidade de ser não-singular (e portanto admitir inversa), e por isso a solução da equação (III-29) é viável.

Vale mencionar que os erros de arredondamento porventura introduzidos não são significativos, uma vez que o objetivo é meramente distinguir entre zeros (0) e uns (1), os bits do texto claro binário. Como A e S são conhecidos pelo criptoanalista, determinar o vetor x torna-se trivial.

III.2.3.2.1.2 - ANÁLISE CRÍTICA

O método apresentado acima é mais elaborado e preciso que a técnica de força bruta, uma vez que o criptoanalista utiliza o conhecimento simultâneo de todos os criptogramas, referentes à mensagem transmitida, e todas as chaves públicas para aplicar a técnica de ataque, em vez de usar apenas um único criptograma e a correspondente chave pública, e então recuperar a mensagem.

Pela própria estrutura e conceituação do método, pode-se afirmar que o mesmo continua válido também para o caso em que a matriz A (matriz de chaves públicas) não é quadrada, ou seja, quando o número de vezes (m) em que a mensagem será transmitida é maior que o número de elementos (n) da chave criptográfica. Isso é verdade porque matrizes retangulares também possuem inversa (à esquerda ou à direita da matriz original). A matriz inversa à esquerda da matriz A é definida como:

$$A_e^{-1} = (A^T . A)^{-1} . A^T$$

onde: A é a matriz retangular original (m x n)
A^T é a matriz transposta de A (n x m)
A_e^{-1} é a matriz inversa à esquerda de A (n x m)

Para que $(A^T . A)$ tenha inversa é necessário que $m \geq n$.

Para a matriz A também vale a propriedade:

$$A_e^{-1} . A = I_n$$

onde I_n é a matriz identidade de dimensão (n x n).

No caso em questão, emprega-se a matriz inversa à esquerda, como segue:

$$S = A \cdot x \quad \rightarrow \quad A_e^{-1} \cdot S = A_e^{-1} \cdot A \cdot x$$

e portanto vem:

$$A_e^{-1} \cdot S = x$$

Deve-se mencionar que a matriz retangular considerada terá mais linhas que colunas, pois do contrário o sistema de equações seria indeterminado (mais incógnitas que equações). É claro que neste caso bastaria considerar a maior matriz quadrada contida na matriz retangular e, então, aplicar o método. Porém, com mais informações, a decifração se torna mais precisa, podendo inclusive "corrigir" eventuais erros de transmissão.

Uma outra observação a respeito do método é que o mesmo pode ser aplicado, também, para vetor mensagem não-binário. Para obter o texto claro original correspondente aos criptogramas transmitidos, bastaria o criptoanalista tomar como solução da multiplicação matricial $A^{-1} \cdot S$ o vetor inteiro mais próximo, a fim de eliminar os erros de arredondamento.

Para concluir a análise, pode-se afirmar que o método de ataque apresentado certamente não chega a ser um perigo para os usuários do sistema criptográfico de chave pública tipo mochila, apenas representa uma restrição ao seu emprego em situações de "broadcast". A fim de evitar este tipo de ataque, os usuários do sistema devem estar atentos para não transmitirem, simultaneamente, a mesma mensagem a vários destinatários (mesmo usando chaves diferentes). Uma sugestão para obter-se "mensagens diferentes" é inserir brancos aleatórios no conteúdo da mensagem original.

III.2.3.2.1.3 - EXEMPLO DE APLICAÇÃO

O sistema mochila apresentado a seguir, transcrito da referência [11], apesar de pequeno demais para ser usado como um criptossistema seguro, serve como exemplo ilustrativo do método descrito acima.

Sejam considerados 10 usuários com as seguintes chaves públicas:

USUÁRIO	CHAVE									
1	1811	1625	1155	1193	1059	1321	1635	1217	1531	1177
2	1171	1433	1651	1361	1603	1905	1651	1465	1227	1473
3	1683	1489	1731	1281	1107	1705	1563	1977	1795	1921
4	1427	1513	1291	1073	1059	1345	1891	1129	1699	1681
5	1795	1641	1635	1633	1379	1225	1587	1553	1275	1081
6	1251	1721	1363	1281	1011	1833	1899	1841	1603	1345
7	1587	1473	1091	1937	1507	1849	1475	1561	1331	1641
8	1051	1537	1763	1339	1787	1721	1595	1785	1891	1281
9	1019	1529	1243	1049	1755	1329	1587	1449	1707	1849
10	1083	1857	1339	1969	1115	1265	1555	1297	1083	1473

Seja também a seguinte mensagem a ser transmitida a esses 10 usuários :

$$x = (1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$$

Consequentemente, os criptogramas a serem enviados aos usuários são :

USUÁRIO	1	2	3	4	5	6	7	8	9	10
CRIPTOGRAMA	8188	8788	10116	8516	8644	8676	9436	9100	8196	8212

cujos valores foram obtidos operando-se a multiplicação matricial $S = A.x$.

Como o criptoanalista conhece as chaves públicas e os criptogramas, ele pode facilmente recuperar a mensagem resolvendo o sistema de equações composto por 10 equações e com 10 incógnitas. Para isso basta calcular a matriz inversa A^{-1} e operar a multiplicação matricial:

$$x = A^{-1} . S$$

Para os valores acima obtém-se:

$A^{-1} . S$ = (1. , -.429153E-04 , 1. , 1.00004 , -.667572E-05 ,
.999964 , .476837E-04 , .858307E-05 , 1.00001 , 1.)

A partir desses valores, não existe dúvida que a mensagem transmitida foi :

x = (1, 0, 1, 1, 0, 1, 0, 0, 1, 1)

III.2.3.2.2 - MÉTODO GRÁFICO

III.2.3.2.2.1 - CARACTERÍSTICAS GERAIS

Muitos criptossistemas de chave pública baseados no problema mochila fazem uso de seqüências supercrescentes e/ou números primos entre si como a informação "trapdoor". Os métodos de ataque apresentados anteriormente [25], [27], [29] e [34] são algoritmos, em tempo polinomial, para resolver os criptossistemas tipo mochila baseados em seqüências supercrescentes. Entretanto, é importante analisar a segurança dos sistemas criptográficos tipo mochila sem considerar a chave secreta, porque os sistemas baseados em números primos não são, em geral, resolvidos por estes métodos, e também existem os criptossistemas que não fazem uso de seqüências supercrescentes. Por isso ITOH, KUROSAWA e TSUJII [54] propuseram um método de ataque aos sistemas mochila de chave pública sem considerar a chave secreta, isto é, analisando os criptogramas para recuperar diretamente o texto claro e não a informação "trapdoor". É um método fácil, baseado na compreensão visual (gráfica) de uma relação entre os valores decimais possíveis para o texto claro e o texto cifrado.

Para uma mochila criptográfica $a = (a_1, a_2, \ldots, a_k)$ pode ser suposto, sem perda de generalidade, que:

$$a_1 < a_2 < \ldots < a_k$$

(A complexidade para ordenar a seqüência é $O(k.\log k)$)

As características principais do método de ataque são apresentadas a seguir.

Para cada texto claro $x = (x_1, x_2, \ldots, x_k)$, associe inteiros não-negativos como segue:

$$X = \sum_{i=1}^{k} x_i \cdot 2^{i-1} \qquad \text{(III-30)}$$

Sejam:

$$X_{i1} = 2^{i-1} \quad , \quad L_i = a_i \qquad \text{(III-31)}$$

$$X_{i2} = 2^i - 1 \quad , \quad U_i = \sum_{j=1}^{i} a_j \qquad \text{(III-32)}$$

$$(1 \leq i \leq k)$$

onde: X é o valor decimal para a mensagem binária representada por $x = (x_1, x_2, \ldots, x_k)$;

L_i é o criptograma para o texto claro X_{i1} ;

U_i é o criptograma para o texto claro X_{i2} .

Considere os gráficos das equações (III-33) e (III-34) mostrados na Figura III-5.

$$Y_1 = L_i \quad ; \quad 2^{i-1} \leq X < 2^i \qquad \text{(III-33)}$$

$$Y_2 = U_i \quad ; \quad 2^{i-1} - 1 < X \leq 2^i - 1 \qquad \text{(III-34)}$$

Todos os pares [texto claro,criptograma] se encontram entre os dois gráficos, sendo que o eixo vertical representa os criptogramas e o eixo horizontal representa os textos claros (expressos, em valor decimal, por X na equação (III-30)). O método de ataque proposto se baseia neste fato.

Teorema III-1 : Seja S o criptograma gerado pela transformação injetiva $f_{(a)} : x \rightarrow S = a.x^T$. Então:

(1) Se $U_{i-1} < S < L_{i+1}$, então $x_i=1$, $x_j=0$ $(i < j \leq k)$

(2) Se $S > U_{k-1}$, então $x_k=1$

(Considerando a seqüência $(a_1,a_2,\ldots,a_k)$ já ordenada).

Para clarear as idéias, segue o exemplo:

Sejam : k = 5

a = (11,19,29,38,85)

S = 78

Determinar x = (x_1,x_2,x_3,x_4,x_5)

Desenhando os dois gráficos Y_1 e Y_2 de acordo com as equações (III-33) e (III-34) obtém-se a Figura III-5, onde S é indicado no eixo vertical.

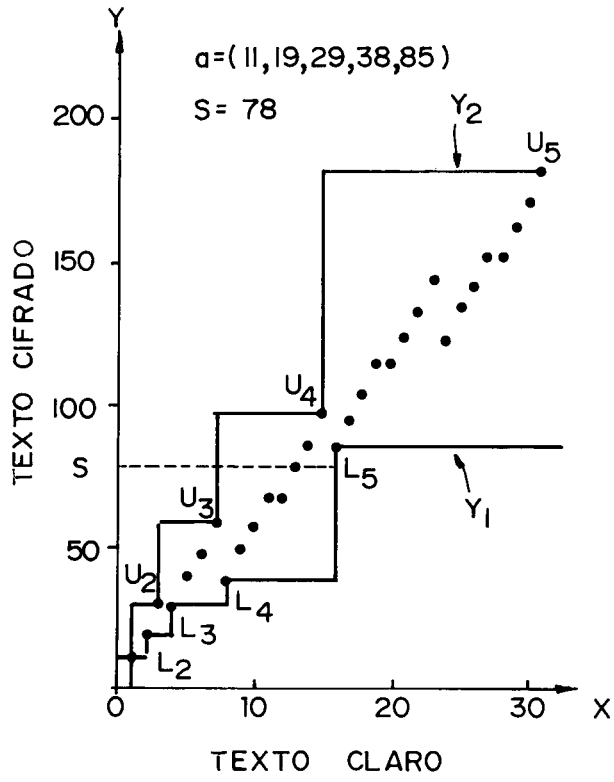


FIGURA III-5: UM EXEMPLO DO TEOREMA III-1

Então obtém-se: $U_3 = 59$, $L_5 = 85$

$$U_3 < S < L_5$$

Pelo Teorema III-1-(1) vem : $x_4=1$ e $x_5=0$

O problema é então reduzido:

$k = 3$

$a_1=11$, $a_2=19$, $a_3=29$

$S' = S - a_4 = 40$

Por um procedimento similar :

$$U_2 = 30$$

$$S' > U_2$$

Pelo Teorema III-1-(2) obtém-se : $x_3=1$

Seguindo o mesmo procedimento vem: $x_1=1$ e $x_2=0$

Consequentemente :

$(x_1,x_2,x_3,x_4,x_5) = (1, 0, 1, 1, 0)$

Deve-se observar que este método fracassa se as condições do Teorema III-1 não forem satisfeitas. Isso ocorre quando $L_i < U_{i-1}$ e S está entre esses dois valores.

É sabido que um problema mochila pode ser facilmente resolvido se:

$$\sum_{j=1}^{n-1} a_j < a_n \qquad (2 \leq n \leq k) \qquad \text{(III-35)}$$

(Esta condição é chamada de supercrescimento).

Os dois gráficos Y_1 e Y_2 deste caso são ilustrados na Figura III-6.

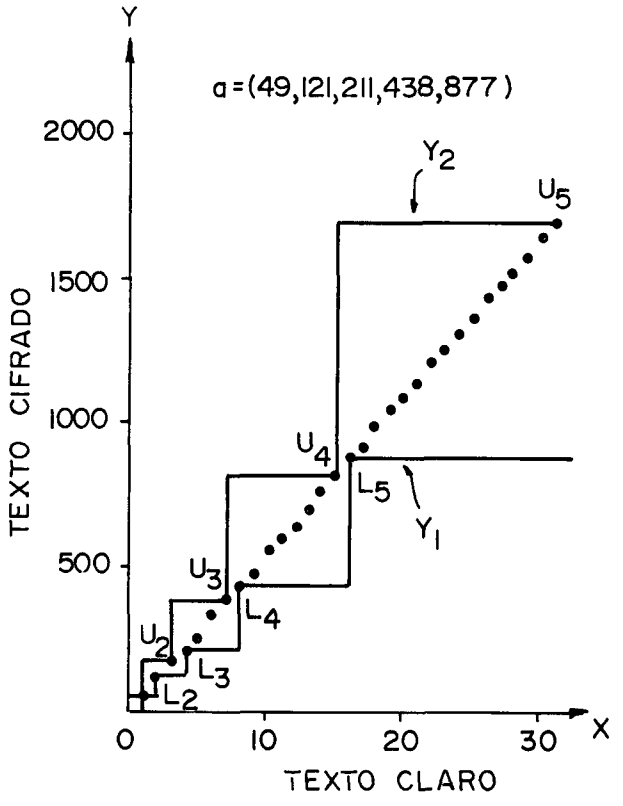


FIGURA III-6: CASO DE SEQÜÊNCIA SUPERCRESCENTE

Pelas equações (III-30), (III-31) e (III-32) é fácil perceber que, para seqüências supercrescentes, as condições do Teorema III-1 são satisfeitas para todos os criptogramas, como pode ser observado na Figura III-6.

O algoritmo de ataque proposto é descrito a seguir , onde S é o valor do criptograma a ser analisado.

Teorema III-2 : O algoritmo de ataque A-1 descrito a seguir é de complexidade O(k).

Prova :

A complexidade dos passos 2 e 3 do algoritmo é O(k).

Seja T o trecho compreendido entre os passos 5 e 14. Toda vez que T é executado, n sempre decresce de mais de 1 unidade. Portanto,o trecho T é executado no máximo k vezes.

Os passos 7, 9 e 13 são executados,no máximo, 1 vez

no algoritmo, e sua complexidade é, no máximo, O(k).

A complexidade dos outros passos do trecho T é inferior (por uma constante) a uma execução deste trecho. Portanto, o algoritmo de ataque A-1 é de O(k).

**

ALGORITMO DE ATAQUE A-1

INÍCIO

1. $U_0 := 0$; $a_{k+1} := \infty$; $n := k$
2. PARA $i := 1$ ATÉ k FAÇA :
3. $x_i := 0$; $U_i := U_{i-1} + a_i$
4. ENQUANTO $n > 0$ FAÇA :
5. SE $S = U_n$ ENTÃO:
6. PARA $j := 1$ ATÉ n FAÇA :
7. $x_j := 1$; $n := 0$
8. SENÃO SE $S = a_n$ ENTÃO:
9. $x_n := 1$; $n := 0$
10. SENÃO SE $S > U_{n-1}$ ENTÃO:
11. SE $S < a_{n+1}$ ENTÃO:
12. $x_n := 1$; $S := S - a_n$; $n := n-1$
13. SENÃO Fracasso ; $n := 0$
14. SENÃO $n := n - 1$

FIM

O Teorema III-3 a seguir generaliza o Teorema III-1.

Teorema III-3 : Se $U_{i-1} < S < L_{t+1}$, $t+1 \leq k$, então:

$$x_{t+1} = x_{t+2} = \ldots = x_k = 0 ,$$

e, pelo menos, um dos elementos entre $x_i, x_{i+1}, \ldots, x_t$ é 1(um).

Prova :

Como $S < L_{t+1}$, então $x_{t+1} = x_{t+2} = \ldots = x_k = 0$.

Como:

$$S > U_{i-1} = \sum_{j=1}^{i-1} a_j$$

então pelo menos um elemento é 1 (um) entre $x_i, x_{i+1}, \ldots, x_t$.

**

O Teorema III-3 é o mesmo que o Teorema III-1 se t=i. O Teorema III-3 aumenta a habilidade de atacar textos cifrados.

Considere o seguinte exemplo:

Sejam : $k = 5$

$a_1=11$, $a_2=19$, $a_3=29$, $a_4=38$, $a_5=85$

$S = 48$

Desenhando os dois gráficos Y_1 e Y_2 , obtém-se a Figura III-7.

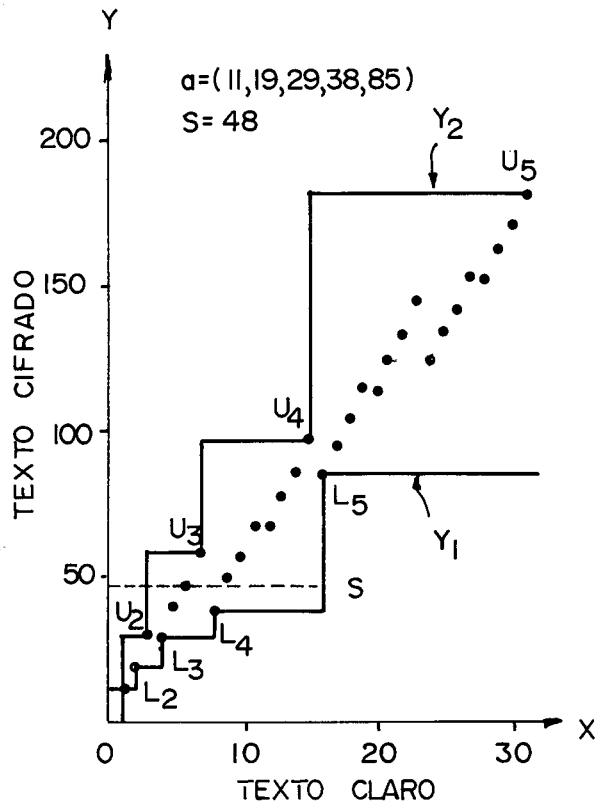


FIGURA III-7: UM EXEMPLO DO TEOREMA III-3

Neste exemplo : $U_2 = 30$, $U_3 = 59$, $S = 48$

$L_4 = 38$, $L_5 = 85$

Como: $U_2 < S < L_5$, pelo Teorema III-3 obtém-se:

$x_5=0$ e pelo menos um elemento é 1 entre x_3 e x_4 .

Primeiramente supor $x_4=1$, então:

$S' = S - a_4 = 10$

Isso significa que a suposição $x_4=1$ é incorreta (porque neste caso S' é menor que o menor a_i). Portanto:

$x_3=1$ e $S' = S - a_3 = 19 = a_2$

e então : $x_1=0$ e $x_2=1$

Consequentemente:

$(x_1,x_2,x_3,x_4,x_5) = (0, 1, 1, 0, 0)$

Este exemplo mostra que a estabilidade do método de ataque é melhorada com a utilização do Teorema III-3; neste caso o método não funcionaria se fosse aplicado o Teorema III-1.

No Teorema III-4 é apresentada uma condição suficiente, mas não necessária (vide Teorema III-3) para resolver o problema mochila em tempo linear, a qual é um pouco mais geral que a bem conhecida propriedade de supercrescimento.

Teorema III-4 : Se

$$\sum_{j=1}^{n-1} a_j - a_1 < a_n \quad (3 \leq n \leq k) \qquad \text{(III-36)}$$

e $a_1 < a_2$, então o problema mochila pode ser resolvido em tempo linear aplicando o algoritmo de ataque proposto A-1 (excluindo o tempo para colocar em ordem crescente os elementos a_i).

Prova :

O algoritmo de ataque A-1 fracassa se existir S tal que:

$L_n < S < U_{n-1}$

ou, usando as equações (III-31), (III-32) e (III-36) :

$$a_n < S < a_n + a_1 \qquad \text{(III-37)}$$

(i) A menos que $x_{n+1}=x_{n+2}= \ldots =x_k = 0$, então:

$$S \geq a_{n+1} > \sum_{j=2}^{n} a_j \geq a_2 + a_n > a_1 + a_n$$

Portanto não existe S satisfazendo a equação (III-37) para a suposição de que pelo menos um $x_i \neq 0$ para $n+1 \leq i \leq k$.

(ii) Suponha que $x_n=x_{n+1}= \ldots=x_k = 0$, então o maior S é U_{n-1} e o segundo maior S é $U_{n-1} - a_1 < a_n$. Portanto não existe S satisfazendo a equação (III-37) para a suposição (ii).

(iii) Suponha que $x_n=1$, $x_{n+1}=x_{n+2}= \ldots =x_k = 0$, então o menor S é a_n e o segundo menor S é $a_n + a_1$. Portanto não existe S satisfazendo a equação (III-37) para a suposição (iii).

Consequentemente, o algoritmo de ataque A-1 sempre funciona se a condição do Teorema III-4 for satisfeita.

**

A Figura III-8 a seguir mostra um problema mochila que satisfaz a condição do Teorema III-4.

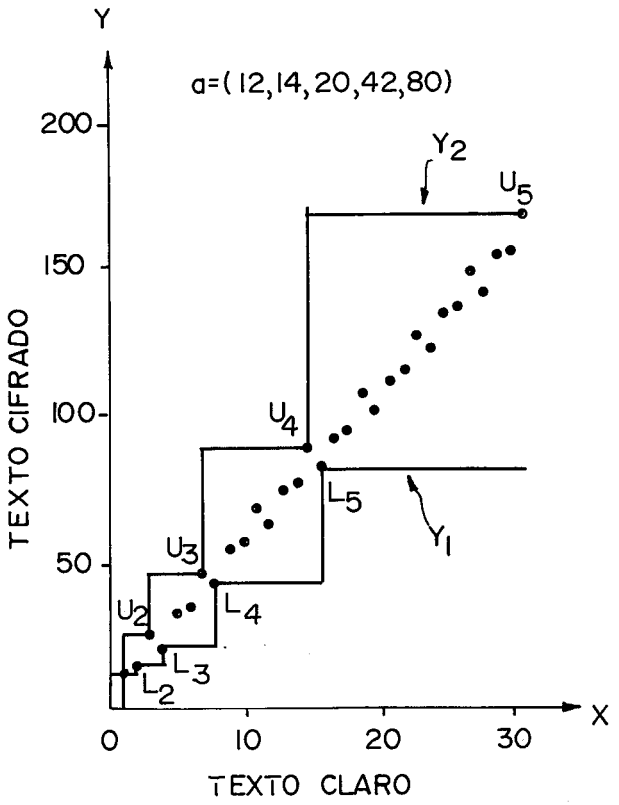


FIGURA III-8: EXEMPLO DO TEOREMA III-4

Teorema III-5 : Se

$$\sum_{j=1}^{n-1} a_j - a_2 < a_n \qquad (3 \leq n \leq k) \qquad \text{(III-38)}$$

e $a_1 < a_2 < a_3$, então o problema mochila pode ser resolvido em tempo linear (excluindo o tempo para colocar em ordem crescente os elementos a_i).

Prova:

Se existir S tal que :

$$S = U_{n-1} - a_1 \qquad \text{(III-39)}$$

então será provado que S é um dos seguintes :

$$L_n < S < U_{n-1} \qquad \text{(III-40)}$$

$$S = L_n + a_1 \qquad \text{(III-41)}$$

Usando as equações (III-31), (III-32) e (III-38) obtém-se, para (III-40) :

$$a_n < S < a_n + a_2 \qquad \text{(III-42)}$$

(i) A menos que $x_{n+1}=x_{n+2}= \ldots =x_k = 0$, então:

$$S \geq a_{n+1} > \sum_{j=1}^{n} a_j - a_2 > a_n + a_3 > a_n + a_2$$

Portanto, não existe S satisfazendo a equação (III-42) para a suposição de que pelo menos um $x_i \neq 0$ para $n+1 \leq i \leq k$.

(ii) Supondo que $x_n=x_{n+1}= \ldots =x_k = 0$, então o segundo maior S é $U_{n-1} - a_1$ e o terceiro maior S é $U_{n-1} - a_2$ (< an). Portanto não existe S satisfazendo a equação (III-42), exceto equação (III-41) para a suposição (ii).

(iii) Supondo que $x_n=1$, $x_{n+1}=x_{n+2}= \ldots =x_k = 0$, então o segundo menor S é $a_n + a_1$ e o terceiro menor S é $a_n + a_2$. Portanto, não existe S satisfazendo a equação (III-42), exceto equação (III-41) para a suposição (iii).

Assim, se existe S satisfazendo a equação (III-39), então tal valor é dado ou pela equação (III-40) ou pela (III-41).

**

Consequentemente, um problema mochila que satisfaz a condição (III-38) pode ser resolvido em tempo linear, utilizando-se uma versão modificada do algoritmo de ataque A-1 proposto.

A Figura III-9 exemplifica o Teorema III-5.

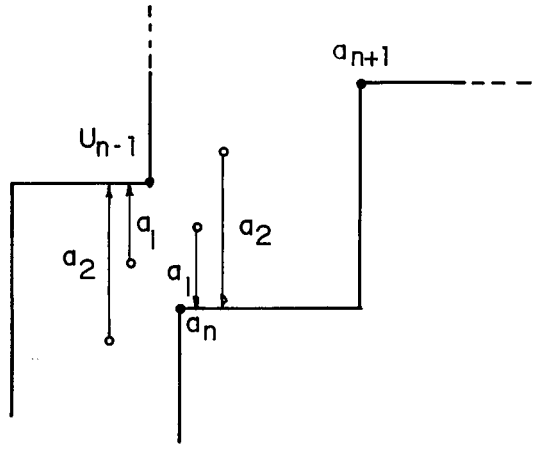


FIGURA III-9 : UM EXEMPLO DO TEOREMA III-5

Deve-se notar que as condições de validade dos Teoremas III-4 e III-5 são mais abrangentes que a propriedade de supercrescimento. Assim sendo, o método de ataque criptoanalítico é mais geral, pois se aplica aos casos de mochilas não supercrescentes que atendem às condições dos Teoremas apresentados acima.

III.2.3.2.2.2 - ANÁLISE CRÍTICA

O método de ataque a criptossistemas mochila apresentado em [54] é um método fácil, e sua grande utilidade é poder "quebrar", em tempo linear, mochilas que não empregam seqüências supercrescentes como informação "trapdoor". A técnica de ataque, conforme ilustrada pelas Figuras III-5 a III-9, utiliza uma relação entre os valores decimais possíveis para os textos claros e para os textos cifrados.

O método se baseia em recuperar, diretamente, o texto claro (representado pela seqüência $x = (x_1, x_2, \ldots, x_n)$), e não a informação "trapdoor", analisando os criptogramas e a chave pública, sem considerar a chave secreta.

Devido às suas características, este método pode ser aplicado a criptossistemas mochila com qualquer informação "trapdoor". Pode, ainda, ser aplicado a criptossistemas mochila de iteração múltipla, desde que satisfaçam às condições de validade dos teoremas.

Na apresentação da técnica de ataque foram evidenciadas , pelos teoremas, as condições suficientes para resolver o problema mochila em tempo linear, as quais são mais gerais que a propriedade de supercrescimento. Isso significa que, para a construção de um criptossistema seguro, devem ser evitadas as condições de validade dos Teoremas III-4 e III-5.

III.2.3.3 - ATAQUE POR REDUÇÕES SUCESSIVAS

III.2.3.3.1 - INTRODUÇÃO

As mochilas supercrescentes são também chamadas de "mochilas solúveis". Uma classe mais ampla de mochilas foi definida por INGERMARSSON [15]: as "mochilas parcialmente solúveis".

Uma mochila é parcialmente solúvel se $a_j > \sum_{i=1, i\neq j}^{n} a_i$ para pelo menos um índice j. (Neste caso a seqüência $a = (a_1, a_2, \ldots, a_n)$ é também chamada de dominada ou seqüência com elemento dominante, no caso o j-ésimo elemento).

Se a seqüência $a = (a_1, a_2, \ldots, a_n)$ for parcialmente solúvel, então pode-se determinar x_j a partir do criptograma S e da chave pública $a = (a_1, a_2, \ldots, a_n)$. Portanto, uma maneira de atacar o criptossistema mochila de chave pública é empregando o Método de Reduções Sucessivas para recuperar a mensagem bit-a-bit. Esse método consiste em determinar parâmetros adequados para transformar, pela multiplicação modular, a chave pública numa "seqüência com elemento dominante".

O primeiro ataque criptoanalítico ao sistema mochila, baseado no método de reduções sucessivas, foi apresentado em 1978 por HERLESTAM [6]. A idéia básica da técnica é obter uma mochila parcialmente solúvel, usando parâmetros adequados, com apenas uma multiplicação modular. Obtida a seqüência dominada, pode-se determinar o bit x_j da mensagem correspondente ao elemento dominante a_j. A mochila é, então, reduzida, removendo-se do criptograma transformado a parcela $x_j.a_j$ e o procedimento é repetido até que toda a mensagem seja recuperada.

Entretanto, nem todas as mochilas são transformadas em mochilas parcialmente solúveis pela multiplicação modular, e, portanto, neste caso o algoritmo proposto em [6] não pode ser aplicado. Uma descrição mais detalhada sobre mochilas transformáveis multiplicativamente é apresentada por INGERMARSSON [15].

Em fins de 1982, DESMEDT, VANDEWALLE e GOVAERTS [21] mostraram como duas transformações modulares iterativas podem facilitar a quebra de mochilas que não podiam ser resolvidas empregando-se apenas uma única transformação modular. A idéia básica da técnica é similar à de HERLESTAM [6], sendo que agora são usadas duas transformações modulares para obter a mochila parcialmente solúvel, isto é, para obter a seqüência com elemento dominante.

Em 1983 INGERMARSSON [26] propôs uma técnica mais elaborada para quebrar o criptossistema mochila de chave pública, também baseada em reduções modulares sucessivas, utilizando-se inteiros adequadamente escolhidos. O problema mochila original é transformado em um sistema de problemas mochila modificados, para o qual pode ser encontrada uma "solução parcial". Assim, o sistema (e, portanto, o problema original) é reduzido dimensionalmente, e o algoritmo é repetido até se obter a solução completa, isto é, até recuperar toda a mensagem.

A seguir são descritas as características gerais de cada uma das técnicas de ataque baseadas no método de reduções sucessivas.

III.2.3.3.2 - CARACTERÍSTICAS DAS TÉCNICAS DE ATAQUE

III.2.3.3.2.1 - TÉCNICA DE HERLESTAM

A idéia básica da técnica de ataque ao criptossistema mochila proposta por HERLESTAM [6] é determinar uma transformação modular, a ser aplicada à chave pública, tal que a seqüência transformada tenha um elemento dominante. Desta forma pode-se determinar facilmente o bit correspondente da mensagem. O processo é repetido e toda mensagem é recuperada bit-a-bit.

Para o criptossistema mochila de chave pública, seja o texto claro uma palavra de n-bits:

$$x = (x_1, x_2, x_3, \ldots , x_n)$$

e seja uma seqüência de inteiros positivos:

$$a = (a_1, a_2, a_3, \ldots , a_n)$$

tal que a função de cifração

$$E(a) : x \rightarrow S = a_1.x_1 + a_2.x_2 + \ldots + a_n.x_n$$

é injetiva.

Seja M um número primo tal que:

$$M > a_1 + a_2 + a_3 + \ldots + a_n$$

e seja w um inteiro tal que :

$$1 < w < M$$

$$(M, w) = 1$$

Então a transformação:

$$T.E(a) = E_{T(a)}$$

$$T(a_j) = w \cdot a_j \pmod{M} \quad , \quad 1 \leq j \leq n$$

é injetiva.

Se a seqüência $(a_i)_{i=1,n}$ for supercrescente, então a função E(a) é facilmente resolvida e espera-se que T(a) seja não supercrescente e, portanto, em geral, difícil de ser resolvida.

Já foi mostrado por alguns autores que o criptossistema mochila é arriscado, devido ao fato de que o mesmo tipo de transformação T que faz T(a) ser não supercrescente quando $(a_i)_{i=1,n}$ é supercrescente, pode fazer T(a) ser supercrescente quando $(a_i)_{i=1,n}$ for não supercrescente.

O esquema de quebra, com grandes chances de sucesso, apresentado por HERLESTAM [6], pode ser definido como :

1º - Seja $(a_i)_{i=1,n}$ não supercrescente e E(a) injetiva.

2º - Escolha um primo M qualquer tal que:

$$M > a_1 + a_2 + a_3 + \ldots + a_n \qquad \text{(III-43)}$$

(Condição de M-dominância)

3º - Escolha um índice j , $1 \leq j \leq n$ e determine w tal que

$$w \cdot a_j \equiv 1 \pmod{M} \qquad \text{(III-44)}$$

4º - Seja $a' = (a'_i)_{i=1,n}$ a mochila transformada:

$$a'_i \equiv w \cdot a_i \pmod{M} \quad , \quad i = 1,\ldots,n \qquad \text{(III-45)}$$

e

$$S' = w \cdot S \pmod{M} \qquad \text{(III-46)}$$

o criptograma transformado.

5º - Se, com uma indexação adequada,

$$a'_n > a'_1 + a'_2 + \ldots + a'_{n-1} \qquad \text{(III-47)}$$

e

$$S' + M > a'_1 + a'_2 + \ldots + a'_{n-1} + a'_n \qquad \text{(III-48)}$$

então (S', a') pode ser chamada de uma redução de (S , a) e x_n é facilmente determinado a partir de (S', a') : se $S' \geq a'_n$, então $x_n = 1$, caso contrário, $x_n = 0$.

6º - O problema mochila reduzido :

$$S' - a'_n.x_n = a'_1.x_1 + \ldots + a'_{n-1}.x_{n-1} \qquad \text{(III-49)}$$

pode ser manipulado com a mesma técnica, escolhendo um outro número primo, etc...

7º - Se, para $j = 1,2,\ldots,n$, o primo M não produzir nenhuma redução de (S , a), escolher um outro valor M e repetir o procedimento.

8º - Ao fim do processamento obter-se-á a seqüência que corresponde ao texto claro : $(x_i)_{i=1,n}$.

Herlestam concluiu, após intensa investigação numérica, ser possível reduzir problemas mochila sucessivamente, não apenas aqueles obtidos por transformação de mochilas supercrescentes, mas também aquelas injetivas não supercrescentes escolhidas aleatoriamente. Desta forma, o método de ataque proposto parece ser eficaz contra o sistema criptográfico tipo mochila.

Para ilustrar a técnica descrita, segue um exemplo numérico, formulado por PAZ DE LIMA [47].

EXEMPLO :

Seja a chave pública $a = (3,5,6,7)$ injetiva não-supercrescente. Para a mensagem $x = (1,1,0,0)$ o criptograma a ser transmitido é $S = 8$.

Aplicando o algoritmo de ataque proposto vem:

- Escolhendo $M = 31$ e $w = 26$, para $j=3$ ($a_3=6$) tem-se:
  $w \cdot a_3 = 1 \bmod 31$ ($156 = 1 \bmod 31$)

- Com a transformação modular obtém-se :

  $a' = (16,6,1,27)$
  $S' = 8 \times 26 \bmod 31 = 22$

- Como $a'_4 = 27 > 16 + 6 + 1 (= 23)$ e
  $S' + M = 22 + 31 = 53 > 16 + 6 + 1 + 27 (= 50)$
  então pode-se determinar o elemento x_4 pois (S', a') é uma redução do problema inicial.
  $S' = 22 < a'_4 = 27 \quad \therefore \quad x_4 = 0$

- Repetindo-se o processo para a mochila reduzida $(a_{r_i})_{i=1,3}$
  $a_r = (16,6,1)$
  $S_r = 22$, vem :

  Para os mesmos parâmetros $M = 31$ e $w = 26$ e tomando $j=2$ ($a_{r_2}=6$) , a mochila transformada será:

  $a'_r = (13,1,26)$ e $S'_r = 14$

  Como esta seqüência é supercrescente permutada, a recuperação dos bits da mensagem torna-se trivial, obtendo-se : $x_3=0$, $x_1=1$, $x_2=1$.

- Assim foi recuperada toda a mensagem : $x = (1,1,0,0)$

III.2.3.3.2.2 - TÉCNICA DE DESMEDT, VANDEWALLE E GOVAERTS

A idéia básica da técnica de ataque proposta por DESMEDT, VANDEWALLE e GOVAERTS [21] é similar à técnica de HERLESTAM [6], sendo que agora são utilizadas duas transformações modulares em vez de uma, para obter a seqüência transformada com elemento dominante.

Como mostrado anteriormente, SHAMIR [27] desenvolveu um algoritmo para quebrar, em tempo polinomial, quase todas as chaves públicas obtidas, com apenas uma transformação secreta, a partir de seqüência supercrescente. Entretanto, ele sugeriu que chaves públicas de cifrar obtidas após várias transformações poderiam ser mais seguras. Pelos resultados apresentados em [38], pode-se afirmar, genericamente, que transformações iterativas podem aumentar, apenas preservar, ou até reduzir o nível de segurança do sistema criptográfico tipo mochila.

No artigo publicado em fins de 1982 DESMEDT, VANDEWALLE e GOVAERTS [21] mostraram como duas transformações iterativas podem facilitar a quebra de criptossistemas mochila.

A técnica de ataque apresentada em [21], em vez de quebrar toda a mensagem, se limita a quebrar apenas um bit, x_j, pois, devido à redundância da mensagem, muitas vezes basta conhecer alguns bits.

Definição III-6 : Uma chave $a = (a_1, a_2, \ldots, a_n)$ é dita j-dominante se, e somente se:

$$a_j > \sum_{i=1, i\neq j}^{n} a_i \quad (\text{ou} \quad 2.a_j > \sum_{i=1}^{n} a_i) \qquad \text{(III-50)}$$

Então x_j pode ser facilmente determinado :

$x_j = 0$ se $S < a_j$

$x_j = 1$ se $S \geq a_j$

A idéia central da técnica de ataque é transformar a seqüência $(a_i)_{i=1,n}$ em uma chave j-dominante. Se isso não for possível com apenas uma transformação, então uma segunda transformação pode ser utilizada para tentar determinar a seqüência dominada.

É possível transformar S e a , por meio da multiplicação por w.(módulo M) , em S' e a' , onde w, M e a_i são inteiros positivos, sendo $0 < S' < M$ e $0 < a'_i < M$.

Para ter-se, ainda, $S' = a' . x^T$, é preciso que seja satisfeita a condição de M-dominância.

Definição III-7 : Uma transformação w.(módulo M) de $(a_i)_{i=1,n}$ em $(a'_i)_{i=1,n}$ é M-dominante se, e somente se:

$$M > \sum_{i=1}^{n} a_i \qquad \text{(III-51)}$$

O resultado principal do estudo apresentado em [21] é sintetizado no teorema a seguir.

Teorema III-8 : Se, para uma dada chave de cifrar $(a_i)_{i=1,n}$ que não possui elemento dominante, existirem um vetor $s = (s_i)_{i=1,n}$ e um inteiro j, $1 \leq j \leq n$, tais que:

$$\max_k \left(s_k / a_k \right) < \frac{(1 + \Sigma s_i)}{\Sigma a_i} \qquad \text{(III-52)}$$

$$\frac{(\Sigma s_i - 2.s_j)}{(\Sigma a_i - 2.a_j)} < \min_\ell \left(s_\ell / a_\ell \right) \qquad \text{(III-53)}$$

então duas transformações M-dominantes convertem a chave $a = (a_i)_{i=1,n}$ em uma chave $a'' = (a''_i)_{i=1,n}$ com elemento dominante (o j-ésimo elemento).

Este teorema apenas garante a existência da chave $(a''_i)_{i=1,n}$, cuja construção a partir de $(s_i)_{i=1,n}$ é mostrada no algoritmo a seguir. Vale ressaltar que a maior dificuldade do método é a obtenção do vetor $(s_i)_{i=1,n}$.

ALGORITMO PARA OBTENÇÃO DA CHAVE COM ELEMENTO DOMINANTE

Passo 1 :

Transformação da seqüência $(a_i)_{i=1,n}$ em $(a'_i)_{i=1,n}$ usando a multiplicação modular * w (mod M) .

- Escolher w e $M > \sum_{i=1}^{n} a_i$, primos entre si, tais que:

$$\max_k \left(s_k / a_k \right) < \frac{w}{M} < \frac{\left(1 + \Sigma s_i \right)}{\Sigma a_i} \qquad \text{(III-54)}$$

- Obter a seqüência $(a'_i)_{i=1,n}$ a partir da seqüência $(a_i)_{i=1,n}$ e do vetor $(s_i)_{i=1,n}$, da forma:

$$a'_i = a_i.w - s_i.M \quad , \quad i = 1,\ldots,n \qquad \text{(III-55)}$$
$$a'_i > 0$$

Passo 2 :

Transformação da seqüência $(a'_i)_{i=1,n}$, na seqüência $(a''_i)_{i=1,n}$ usando a segunda transformação modular * w' (mod M') .

- Calcular os inteiros w^{-1} , P e $(s'_i)_{i=1,n}$:

w^{-1} tal que : $w^{-1}.w = 1 \bmod M$; (III-56)

$P = (w.w^{-1} - 1)/M$; (III-57)

$s'_i = a_i.P - s_i.w^{-1}$, $i = 1,\ldots,n$ (III-58)

- Escolher w' e M' , primos entre si, tais que:

$$\max_k \left(s'_k / a'_k \right) < \frac{w'}{M'} < \frac{\left(\Sigma s'_i - 2.s'_j \right)}{\left(\Sigma a'_i - 2.a'_j \right)} \qquad \text{(III-59)}$$

- Obter a chave $(a''_i)_{i=1,n}$ com elemento dominante :

$$a''_i = a'_i.w' - s'_i.M' \quad , \quad i = 1,\ldots,n \qquad \text{(III-60)}$$

Para qualquer criptograma específico S , as transformações processadas acima produzem S" , a partir do qual o j-ésimo bit da mensagem pode ser facilmante determinado usando-se a propriedade de j-dominância da seqüência obtida após as duas transformações modulares.

Para qualquer vetor $(s_i)_{i=1,n}$ satisfazendo as equações (III-52) e (III-53), o algoritmo determina w , M , w' e $(a''_i)_{i=1,n}$ em tempo polinomial em função do tamanho n do vetor $(a_i)_{i=1,n}$.

A maior dificuldade do método de ataque é determinar $(s_i)_{i=1,n}$ satisfazendo as equações (III-52) e (III-53) , que é um problema de programação inteira. Para n fixo, um algoritmo em tempo polinomial é apresentado por LENSTRA [48].

É importante ter em mente que a utilização de transformações iterativas da mochila para propósitos criptográficos, nem sempre aumenta a segurança do sistema, podendo, inclusive, facilitar a sua quebra.

A seguir é apresentado um exemplo ilustrativo da técnica de ataque proposta.

EXEMPLO :

Considere a seguinte chave de cifrar:

$a = (2,5,13,19)$

a qual não possui elemento dominante.

O algoritmo apresentado anteriormente produz uma chave $a'' = (a''_1, a''_2, a''_3 , a''_4)$, com elemento dominante, para decifrar, pelo menos, um bit da mensagem.

Para o vetor $s = (1,3,8,12)$ e para $j=4$ é fácil verificar que são satisfeitas as condições das equações (III-52) e (III-53).

$$\max_k (s_k / a_k) = \max (1/2;3/5;8/13;12/19) = 12/19$$

$$\frac{1 + \Sigma s_i}{\Sigma a_i} = \frac{1 + (1+3+8+12)}{(2+5+13+19)} = \frac{25}{39}$$

$$\frac{\Sigma s_i - 2.s_j}{\Sigma a_i - 2.a_j} = \frac{24 - 2 \times 12}{39 - 2 \times 19} = 0$$

$$\min_\ell (s_\ell / a_\ell) = \min (1/2;3/5;8/13;12/19) = 1/2$$

$$12/19 < 25/39 \qquad e \qquad 0 < 1/2$$

Aplicando o algoritmo vem :

Passo 1 :

- Escolher w e M > 39 , primos tais que:

  12/19 < w/M < 25/39

  Por exemplo : M = 101 e w = 64

- Obter a seqüência $a'_i = a_i.w \pmod{M}$, i=1,...,4 :

  a = (2,5,13,19) , M = 101 e w = 64

  ↓

  a' = (27,17,24,4)

Passo 2 :

- Usando $w^{-1} \bmod M$ e P , obter o vetor $(s'_i)_{i=1,4}$:

  $w^{-1} = w^{(M-2)} . \bmod M = 64^{99} \bmod 101 = 30$

  P = (64 x 30 - 1)/ 101 = 19

  $s'_i = a_i.P - s_i.w^{-1}$, i=1,...,4

  s' = (8,5,7,1)

- Escolher w' e M' primos entre si tais que:

  8/27 < w'/M' < 19/64

  Por exemplo : M' = 401 e w' = 119

- Obter a chave com elemento dominante :

  $a''_i = a'_i.w' - s'_i.M'$, i=1,...,4

  a" = (5,18,49,75)

  Neste caso a chave obtida é também supercrescente !

III.2.3.3.2.3 - TÉCNICA DE INGEMARSSON

A técnica de ataque ao criptossistema mochila de chave pública apresentada por INGEMARSSON [26], é baseada em reduções modulares sucessivas utilizando-se inteiros adequadamente escolhidos, que transformam o problema mochila original em um sistema de problemas mochila modificados. Freqüentemente pode ser encontrada uma "solução parcial" para este sistema, e então o sistema e o problema originais podem ser reduzidos dimensionalmente e o algoritmo repetido, até obter-se a solução completa.

Segundo [26], ainda não se pode caracterizar formalmente a classe de problemas mochila para a qual o algoritmo de ataque apresentado a seguir seja eficaz. Existem indicações, entretanto, de que a maioria dos problemas mochila que admitem uma única solução (mochilas injetivas) pode ser resolvida pelo uso do referido algoritmo.

O ALGORITMO DE ATAQUE

O problema mochila é determinar o vetor binário desconhecido $x = (x_i)_{i=1,n}$ em (III-61) :

$$S_0 = \sum_{j=0}^{n} a_{0j} \cdot x_j \qquad \text{(III-61)}$$

onde $x_j \in \{ 0,1 \}$ e $a_0 = (a_{00}, \ldots , a_{0n})$ é um vetor inteiro.

Em geral (III-61) pode ter qualquer número de soluções para o vetor $x = (x_i)_{i=1,n}$. Entretanto será analisado apenas o caso em que (III-61) tem somente uma única solução (sistema injetivo). A equação (III-61) pode ser reduzida módulo um inteiro ℓ_{11} escolhido, obtendo-se :

$$S_1 = S_0 - \left\lfloor \frac{S_0}{\ell_{11}} \right\rfloor \ell_{11} = \sum_{j=0}^{n} a_{1j} \cdot x_j + \ell_{11} \cdot y_1$$

onde:

$$y_1 = \left\{ \sum_{j=0}^{n} x_j \cdot \left\lfloor \frac{a_{0j}}{\ell_{11}} \right\rfloor \right\} - \left\lfloor \frac{S_0}{\ell_{11}} \right\rfloor$$

Por reduções sucessivas obtém-se o sistema de equações :

$$S_i = \sum_{j=0}^{n} a_{ij} \cdot x_j + \sum_{j=1}^{i} \ell_{ij} \cdot y_j \qquad \text{(III-62)}$$

onde :

$S_i = S_{i-1} \bmod \ell_{ii}$ para $i > 0$

$a_{ij} = a_{i-1,j} \bmod \ell_{ii}$ para $i > 0$

$\ell_{ij} = \ell_{i-1,j} \bmod \ell_{ii}$ para $j \leq i$

$\ell_{ij} = 0$ para $j > i$

$$y_i = \sum_{j=1}^{i-1} \left\lfloor \frac{\ell_{i-1,j}}{\ell_{ij}} \right\rfloor y_j + \sum_{j=0}^{n} \left\lfloor \frac{a_{i-1,j}}{\ell_{ii}} \right\rfloor x_j - \left\lfloor \frac{S_{i-1}}{\ell_{ii}} \right\rfloor \qquad \text{(III-63)}$$

Resolvendo y_i em (III-62) vem :

$$y_i = - \sum_{j=0}^{n} b_{ij} \cdot x_j + z_i \qquad \text{para } i > 0 \qquad \text{(III-64)}$$

onde :

$$b_{ij} = \frac{a_{ij}}{\ell_{ii}} - \sum_{v=1}^{i-1} \frac{\ell_{iv}}{\ell_{ii}} \cdot b_{vj}$$

$$z_i = \frac{S_i}{\ell_{ii}} - \sum_{v=1}^{i-1} \frac{\ell_{iv}}{\ell_{ii}} \cdot z_v$$

Apesar de (III-61) ter apenas uma única solução, (III-62) e (III-64) podem ter mais de uma solução inteira para y_i com $x_j \in \{0,1\}$. Apenas uma dessas soluções, entretanto, satisfará (III-63).

A idéia básica do algoritmo é usar o fato de que x_j é limitado ao intervalo [0,1] (de fato $x_j \in \{0,1\}$) para limitar y_i usando (III-63) e (III-64) . Provavelmente, existirá apenas um inteiro y_i (para algum "i") no intervalo encontrado. Os valores calculados y_i são inseridos em (III-64) e alguns x_j são encontrados usando a mesma técnica de limite. Então, o número de variáveis desconhecidas x_j em (III-61) é reduzido. O problema mochila é , então, reformulado para um de dimensão menor, e o algoritmo é repetido.

De (III-64) pode-se derivar uma relação recursiva para y_i : multiplica-se (III-64) por ℓ_{iv}/ℓ_{ii} e aplica-se o somatório para "v" variando de 1 a i-1, o que fornece:

$$\sum_{v=1}^{i-1} \frac{\ell_{iv}}{\ell_{ii}} \cdot y_v = - \sum_{j=0}^{n} \left\{ \sum_{v=1}^{i-1} \frac{\ell_{iv}}{\ell_{ii}} \cdot b_{vj} \right\} x_j + \sum_{v=1}^{i-1} \frac{\ell_{iv}}{\ell_{ii}} \cdot z_v$$

observa-se que :

$$\sum_{v=1}^{i-1} \frac{\ell_{iv}}{\ell_{ii}} \cdot b_{vj} = \frac{a_{ij}}{\ell_{ii}} - b_{ij}$$

e

$$\sum_{v=1}^{i-1} \frac{\ell_{iv}}{\ell_{ii}} \cdot z_v = \frac{S_i}{\ell_{ii}} - z_i$$

Assim,

$$\sum_{v=1}^{i-1} \frac{\ell_{iv}}{\ell_{ii}} \cdot y_v = - \sum_{j=0}^{n} \frac{a_{ij}}{\ell_{ii}} \cdot x_j +$$

$$+ \sum_{j=0}^{n} b_{ij} . x_j - z_i + \frac{S_i}{\ell_{ii}}$$

É facilmente reconhecido y_i de (III-64) no lado direito da expressão acima. Isso, finalmente, fornece :

$$y_i = -\sum_{j=0}^{n} \frac{a_{ij}}{\ell_{ii}} \cdot x_j + \frac{S_i}{\ell_{ii}} - \sum_{v=1}^{i-1} \frac{\ell_{iv}}{\ell_{ii}} \cdot y_v \qquad \text{(III-65)}$$

Como observado anteriormente, (III-65) pode ter múltiplas soluções (inteiros y_i e $x_j \in \{0,1\}$) devido às reduções modulares para obter (III-62). Para encontrar uma única solução, é preciso usar as relações (III-63) e (III-65).

OS LIMITES DE y_i

Usando o fato de que $x_j \in \{0,1\}$, serão determinados os limites para y_i .

Observa-se que a_{ij} e ℓ_{ij} são não-negativos para todo "i" e "j", enquanto b_{ij} pode ter qualquer sinal. Esta observação, usada em (III-63), (III-64) e (III-65), fornece :

$$\text{máx } y_i = \left\lfloor \text{mín} \left\{ \begin{array}{l} z_i - \sum b_{ij} \quad , j \text{ tal que } b_{ij} < 0 \\ \\ \dfrac{S_i}{\ell_{ii}} - \displaystyle\sum_{v=1}^{i-1} \frac{\ell_{iv}}{\ell_{ii}} \cdot (\text{min } y_v) \\ \\ \displaystyle\sum_{v=1}^{i-1} \left\lfloor \frac{\ell_{i-1,j}}{\ell_{ii}} \right\rfloor \cdot (\text{máx } y_i) + \sum_{j=0}^{n} \left\lfloor \frac{a_{i-1,j}}{\ell_{ii}} \right\rfloor - \left\lfloor \frac{S_{i-1}}{\ell_{ii}} \right\rfloor \end{array} \right. \right\rfloor ,$$

para obter, entre os valores máximos possíveis de y_i , o menor valor.

$$\text{mín } y_i = \left\lceil \text{máx} \left\{ \begin{array}{l} z_i - \sum b_{ij} \quad , \; j \text{ tal que } b_{ij} > 0 \\ -\sum_{j=0}^{n} \frac{a_{ij}}{\ell_{ii}} + \frac{S_i}{\ell_{ii}} - \sum_{v=1}^{i-1} \frac{\ell_{iv}}{\ell_{ii}} \cdot (\text{máx } y_v) \\ \sum_{v=1}^{i-1} \left\lfloor \frac{\ell_{i-1,j}}{\ell_{ii}} \right\rfloor \cdot (\text{mín } y_i) - \left\lfloor \frac{S_{i-1}}{\ell_{ii}} \right\rfloor \end{array} \right. \right\rceil ,$$

para obter, entre os valores mínimos possíveis de y_i , o maior valor.

Nota : $\lceil \theta \rceil$ denota o menor inteiro $\geq \theta$
$\lfloor \theta \rfloor$ denota o maior inteiro $\leq \theta$

A parte mais importante no limite definido acima é a baseada em (III-64) usando o coeficiente b_{ij}. Então, para restringir o intervalo de variação de y_i , deve-se usar a seguinte regra:

Escolher ℓ_{ii} para minimizar $\sum_{j=0}^{n} \lvert b_{ij} \rvert$.

O desempenho do algoritmo usando esta regra é ainda uma questão em aberto. A experiência indica, entretanto, que a partir da quarta iteração ($i \geq 4$) só deve existir um único valor inteiro para y_i , como descrito em [26].

Uma vez determinados alguns valores y_i , eles podem ser usados em (III-64) para compor um sistema de equações. A partir desse sistema, o mesmo número de elementos x_j pode ser obtido com a mesma técnica de limite empregada para determinar os valores de y .

III.2.3.3.3 - ANÁLISE CRÍTICA

As três técnicas de ataque ao criptossistema mochila, descritas acima, utilizam o método de reduções sucessivas para recuperar a mensagem. Uma propriedade importante dessas técnicas é que analisam a chave pública, e também o criptograma, para determinar os parâmetros adequados da(s) transformação(ções) modular(es) a ser(em) empregada(s) na obtenção da seqüência "parcialmente solúvel" (ou seqüência com elemento dominante).

A característica básica da técnica de HERLESTAM [6] é tentar obter uma seqüência com elemento dominante usando apenas uma multiplicação modular M-dominante. O método pode ser usado para reduzir sucessivamente não apenas os problemas mochila obtidos por transformação de mochilas supercrescentes, mas também aquelas mochilas injetivas não-supercrescentes escolhidas aleatoriamente. No entanto, uma fraqueza do método é que a obtenção dos parâmetros da multiplicação modular (w e M) é feita por tentativa, isto é, determinam-se os parâmetros e depois verificam-se as condições impostas pelo algoritmo. Se elas não forem satisfeitas, são calculados novos parâmetros e abandonados os antigos.

A técnica de DESMEDT, VANDEWALLE e GOVAERTS [21] tenta obter a seqüência com elemento dominante utilizando duas multiplicações modulares M-dominantes. A dificuldade maior do algoritmo é a obtenção do vetor $(s_i)_{i=1,n}$, usado nas equações das condições a serem satisfeitas pelos parâmetros da transformação modular. Uma limitação de emprego do método é a sua utilidade somente para valores pequenos de n (mochilas pequenas), pois para n grande o desempenho do algoritmo é piorado.

A técnica de INGEMARSSON [26], basicamente, transforma o problema mochila original a ser resolvido em um sistema de problemas mochila modificados usando transformações modulares sucessivas com módulos inteiros adequadamente escolhidos (só utiliza um parâmetro, o módulo). Ainda não se pode caracterizar a classe de problemas mochila para a qual o algoritmo seja eficaz. Existem indicações, entretanto, de que a maioria dos problemas mochila injetivos pode ser resolvida rapidamente pelo uso desse algoritmo.

Os métodos de ataque apresentados em [6], [21] e [26] possuem a vantagem de poderem ser empregados para resolver tanto sistemas mochila de iteração simples como sistemas mochila de iteração múltipla. Ainda, podem ser adaptados de forma a resolverem, também, mochilas não-binárias.

As técnicas descritas devem ser consideradas à luz da controvérsia sobre a segurança do algoritmo mochila de chave pública. Em [38] foi mostrado que a segurança de uma mochila pode não ser aumentada pelo uso de mais de uma transformação modular, e em [21] que a iteração dupla se constitui numa ferramenta forte para quebrar o criptossistema mochila. A procura por tais transformações está fundamentada na análise da chave pública.

Conseqüentemente, aumentam cada vez mais as dúvidas se realmente existem mochilas seguras e como elas podem ser construídas. Enquanto a questão da segurança do criptossistema mochila não é respondida positivamente, é importante lembrar que a utilização de transformações iterativas da mochila para propósitos criptográficos nem sempre aumenta a segurança do sistema, podendo, inclusive, facilitar a sua quebra.

III.2.3.4 - ATAQUE A MOCHILAS DE BAIXA DENSIDADE

III.2.3.4.1 - INTRODUÇÃO

O sistema de chave pública tipo mochila proposto por MERKLE e HELLMAN [3] caracteriza-se por ser um sistema de baixa densidade.

A densidade, d(a), de um sistema mochila binário com a chave pública $a = (a_1, a_2, \ldots, a_n)$ é definida como :

$$d(a) = \frac{n}{\log_2 \max_i \{ a_i \}} \qquad \text{(III-66)}$$

onde: n é o número total de bits usados para transmitir o bloco da mensagem (texto claro) - que, no caso de sistema binário, é o número de elementos da mochila;

$a = (a_1, a_2, \ldots, a_n)$ é a chave pública.

Em termos quantitativos, um sistema mochila é considerado de baixa densidade se $d(a) < 1/\log_2 n$ (o que corresponde a ter-se $a_{i_{máx}} = n^n$).

Um dos tipos de ataque ao criptossistema mochila de chave pública, como mostrado em [25], [27] e [29], baseia-se na recuperação da informação "trapdoor" para poder decifrar as mensagens criptografadas. BRICKELL [35] e LAGARIAS-ODLYZKO [43] propuseram métodos de ataque diferentes. A idéia básica dos algoritmos apresentados por estes autores é tentar determinar diretamente uma solução viável $x = (x_1, x_2, \ldots, x_n)$ para o problema mochila, em vez de recuperar a informação "trapdoor", atacando os elementos da chave pública e o criptograma.

A técnica de Brickell se baseia em determinar n-1 mapeamentos modulares independentes de soma pequena (definidos mais adiante), usando o algoritmo L^3 de redução de base, para serem aplicados aos elementos da mochila e, a partir daí, obter a solução para qualquer criptograma, usando cálculo matricial.

Na técnica de Lagarias-Odlyzko, basicamente, o problema de determinar a solução da mochila é convertido no problema de determinar um vetor particular pequeno não-nulo num reticulado e, então, utilizar o algoritmo L^3 para encontrar este vetor, que é a solução procurada.

Para o propósito desta tese, basta saber que o algoritmo L^3 [50] de redução de base é usado para determinar o menor vetor não-nulo num reticulado, que é o vetor solução.

Um subconjunto de pontos L em $\mathbb{R}^n$ é um reticulado de posto n se $L = \{ \sum_{i=1}^{n} Z_i . v_i : Z_i \in \mathbb{Z} \}$, onde $V_1, \ldots, V_n$ é um conjunto de vetores independentes em $\mathbb{R}^n$ que formam a base de L . O algoritmo L^3 determina uma base reduzida para o reticulado L e, consequentemente, determina o menor vetor nesta base reduzida [48].

Os métodos desenvolvidos por BRICKELL [35] e LAGARIAS-ODLYZKO [43] se constituem num ataque, em tempo polinomial , aos criptossistemas de chave pública tipo mochila. Ambas as técnicas de ataque utilizam o algoritmo L^3 para redução de base de reticulado [50], e se aplicam apenas às mochilas de baixa densidade, isto é, aos criptossistemas que transmitem informação numa taxa inferior à densidade crítica. (É considerada densidade crítica, d_c , função do tamanho da mochila , o valor limite para a densidade de um sistema mochila acima do qual as técnicas de ataque não funcionam. Este valor típico é diferente para cada uma das técnicas de ataque.)

Nas seções subseqüentes são apresentadas as características básicas de cada uma dessas técnicas.

III.2.3.4.2 - CARACTERÍSTICAS GERAIS DOS MÉTODOS

III.2.3.4.2.1 - MÉTODO DE BRICKELL

Foram descritos por BRICKELL [35] dois métodos para resolver mochilas de baixa densidade : o Método 1 é uma técnica para resolver "quase todas" as mochilas de densidade menor que $1/\log_2 n$; o Método 2 é uma técnica ligeiramente diferente para resolver "quase todas" as mochilas de densidade significativamente maior que $1/\log_2 n$.

Antes de passar à descrição dos métodos, alguns conceitos e teoremas serão apresentados para facilitar a compreensão do texto.

Definição III-9 : Mapeamento Modular de Soma Pequena (MMSP): Um mapeamento por $w \bmod M$ da seqüência $a = (a_1, a_2, \ldots, a_n)$ na seqüência $b = (b_1, b_2, \ldots, b_n)$ é dito ter a propriedade de soma pequena se, e somente se,

$$\sum_{i=1}^{n} | b_i | < M \qquad \text{(III-67)}$$

onde b_i é o menor inteiro em valor absoluto tal que :

$$b_i \equiv a_i . w \bmod M \quad , \quad i=1,\ldots,n \qquad \text{(III-68)}$$

Será usada a notação MMSP para referenciar um mapeamento modular com a propriedade de soma pequena.

Teorema III-10 : Suponha que um mapeamento modular por w mod M de $a_1,\ldots,a_n$ em $b_1,\ldots,b_n$ tem a propriedade de soma pequena.

Seja:

$$B = \sum_{i=1}^{n} b_i \qquad \text{(III-69)}$$

$b_i \gg 0$

Suponha que $\sum_{i=1}^{n} x_i.a_i = S$ para algum vetor binário $(x_1,x_2,\ldots,x_n)$.

Seja : $S' = S.w \bmod M$ (III-70)

Seja também :

$$S'' = \begin{cases} S' & \text{se } S' \leq B \\ S' - M & \text{se } S' > B \end{cases}$$

Então :

$$S'' = \sum_{i=1}^{n} x_i.b_i \qquad \text{(III-71)}$$

(A prova do Teorema III-10 encontra-se na referência [35]).

Diz-se que a seqüência $((w_1,M_1),\ldots,(w_k,M_k))$ de MMSP's é $(a_1,a_2,\ldots,a_n)$-independente se os vetores $(a_1,a_2,\ldots,a_n)$, $(a_1w_1 \bmod M_1, a_2w_1 \bmod M_1,\ldots,a_nw_1 \bmod M_1)$,..., $(a_1w_k \bmod M_k, a_2w_k \bmod M_k,\ldots, a_nw_k \bmod M_k)$ forem linearmente independentes.

Teorema III-11 : Se uma seqüência de $n - 1$ MMSP's $(a_1,a_2,\ldots,a_n)$-independentes puder ser determinada, então o problema mochila para o vetor $(a_1,\ldots,a_n)$ pode ser resolvido para qualquer inteiro S_0, computando-se n multiplicações modulares e multiplicando-se uma matriz n x n por um vetor.

Prova :

Seja $((w_1,M_1), \ldots , (w_{n-1},M_{n-1}))$ uma seqüência de n-1 MMSP's $(a_1,a_2,\ldots,a_n)$-independentes.

$$Y = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 w_1 \bmod M_1 & a_2 w_1 \bmod M_1 & \cdots & a_n w_1 \bmod M_1 \\ \vdots & & & \\ a_1 w_{n-1} \bmod M_{n-1} & a_2 w_{n-1} \bmod M_{n-1} & \cdots & a_n w_{n-1} \bmod M_{n-1} \end{bmatrix}$$

Dado um inteiro S_0 , deseja-se determinar um vetor binário $\alpha = (\alpha_1,\ldots,\alpha_n)$ tal que:

$$\sum_{i=1}^{n} \alpha_i . a_i = S_0 \qquad \text{(III-72)}$$

ou mostrar que tal vetor não existe.

Suponha que existe um vetor binário satisfazendo a equação (III-72). Pelo Teorema III-10 pode-se determinar S_1, $S_2,\ldots, S_{n-1}$ tais que :

$$\sum_{i=1}^{n} \alpha_i . (a_i . w_j \bmod M_j) = S_j \quad , \quad 1 \leq j \leq n-1 \qquad \text{(III-73)}$$

$$S_1 = S_0 . w_1 \bmod M_1$$

$$S_2 = S_0 . w_2 \bmod M_2 \qquad \text{(III-74)}$$

$$\vdots$$

$$S_j = S_0 . w_j \bmod M_j$$

Seja $S = (S_0, S_1, \ldots , S_{n-1})$

$$Y . \alpha = S \qquad \text{(III-75)}$$

$$Y^{-1} . S = \alpha \qquad \text{(III-76)}$$

(A matriz Y^{-1} existe porque as linhas da matriz Y são linearmente independentes.)

Desta forma, para resolver o problema mochila para a soma S_0 dada, constrói-se o vetor S como mostrado em (III-74). Se $Y^{-1}.S$ não for um vetor binário, então o problema não tem solução. Se $Y^{-1}.S = \alpha$ for um vetor binário, então calcula-se $\alpha . a$. Se $\alpha . a = S_0$, então α é uma solução, e se $\alpha . a \neq S_0$, então o problema não tem solução.

**

==== MÉTODO 1 ====

Dados os elementos $a_1, a_2, \ldots, a_n$, pode-se empregar o algoritmo L^3 de redução de base no reticulado L em $\mathbb{R}^n$ gerado pelos vetores :

$$\begin{matrix} (1, na_2, na_3, \ldots , \ldots, na_n) \\ (0, na_1, 0 , \ldots , 0 , 0) \\ \vdots \\ (0, 0 , 0 , \ldots , 0 , na_1) \end{matrix} \qquad \text{(III-77)}$$

Proposição III-12 : Seja $v = (v_1,\ldots,v_n)$ um vetor em L. Se :

$$\sum_{i=2}^{n} | v_i | < n.a_1 \quad ,$$

então o mapeamento modular de $a_1, \ldots, a_n$ por $v_1 \bmod a_1$ tem a propriedade da soma pequena.

Prova :

Como v é uma combinação linear inteira dos vetores em (III-77), existem inteiros $y_1, y_2, \ldots, y_n$ tais que :

$$v_1 = y_1$$

$$v_i = y_i.na_1 + y_1.na_i \quad \text{para} \quad 2 \leq i \leq n$$

Como $n|v_i$, $2 \leq i \leq n$ (isto é, v_i é múltiplo de n para $2 \leq i \leq n$), seja $v_i' = v_i/n$ para $2 \leq i \leq n$.

$$v_i' \equiv a_i.y_1 \bmod a_1 \quad \text{para} \quad 2 \leq i \leq n$$

$$0 \equiv a_1.y_1 \bmod a_1$$

Uma vez que $\sum_{i=1}^{n} | v_i' | < a_1$ (pois, por hipótese, $\sum_{i=1}^{n} | v_i | < n.a_1$), o mapeamento modular por $v_1 \bmod a_1$ tem a propriedade da soma pequena.

**

Definição III-13 : Para um vetor $v = (v_1, v_2, \ldots, v_n)$ no reticulado L, sejam $v_1' = 0$, $v_i' = v_i/n$ para $2 \leq i \leq n$ e $v' = (v_1', v_2', \ldots, v_n')$. O vetor v é dito ser suficientemente pequeno se $\sum_{i=2}^{n} | v_i' | < a_1$.

Proposição III-14 : Seja B_L uma base reduzida de L. Se todos os vetores em B_L forem suficientemente pequenos, então podem-se determinar n - 1 MMSP's $(a_1, \ldots, a_n)$-independentes.

Prova :

Sejam $V_1, \ldots, V_n$ vetores na base reduzida B_L . Como $V_1, \ldots, V_n$ são independentes, existe, nesta base, um conjunto de n-1 vetores $V_1', \ldots, V_{n-1}'$ que são independentes (não necessariamente $V_i = V_i'$). Seja Z_i a primeira coordenada de V_i' . Então $(Z_1, a_1), \ldots, (Z_{n-1}, a_1)$ é um conjunto de n - 1 MMSP's para $(a_1, \ldots, a_n)$.

**

Segundo BRICKELL [35], para avaliar a probabilidade de sucesso do Método 1 , deve-se estimar o número de soluções inteiras $y_1, y_2, \ldots, y_n$ para

$$\left| a_i \cdot y_1 + y_i \cdot a_1 \right| \leq \frac{a_1}{n} \quad , \quad 2 \leq i \leq n$$

$$0 < y_1 < a_1 \qquad \text{(III-78)}$$

A região em $\mathbb{R}^n$ definida por (III-78) é um paralelepípedo de 2^n vértices com volume igual a $a_1.(2/n)^{n-1}$. Numa região de volume V, o número esperado de pontos inteiros é V , então o número de soluções inteiras para (III-78) pode ser estimado por $a_1.(2/n)^{n-1}$.

Se $a_1 \cong n^n$, então o número esperado de soluções é igual a $n.2^{n-1}$. Portanto, se a densidade da mochila for menor que $1/\log_2 n$ (o que corresponde a ter-se $a_{i_{máx}} = n^n$), então espera-se que o Método 1 funcione.

==== MÉTODO 2 ====

Se a densidade da mochila for maior que $1/\log_2 n$, não se pode garantir que o Método 1 funcione. O que se pode fazer é diminuir artificialmente a densidade da mochila. Não se pode esperar que isso funcione em todos os casos, mas obter-se-á sucesso sob certas condições.

Dado o vetor $(a_1, \ldots, a_n)$ de densidade maior que $1/\log_2 n$, escolher M e $w < M$ tais que $n^n < M < 2.n^n$ e $(w, M) = 1$.

Seja :

$$b_i \equiv a_i . w \bmod M \quad , \qquad 1 \leq i \leq n \qquad \text{(III-79)}$$

tal que b_i é o menor resíduo não-negativo.

Se, para os valores escolhidos w e M, a densidade de $(b_1, \ldots, b_n)$ for menor que $1/\log_2 n$, então o Método 1 pode ser utilizado para esta mochila de baixa densidade.

Uma vez que os elementos $b_1, \ldots, b_n$ não foram aleatoriamente escolhidos, não se pode mostrar que o Método 1 funcione. Entretanto, se o Método 1 obtiver sucesso para os elementos $b_1, \ldots, b_n$, então pode-se resolver o problema com os elementos $a_1, \ldots, a_n$ e qualquer soma S, usando a informação "trapdoor" w, M.

Se existir um vetor binário $\alpha = (\alpha_1, \ldots, \alpha_n)$ tal que:

$$\sum_{i=1}^{n} \alpha_i . a_i = S \quad , \qquad \text{(III-80)}$$

então tem-se que:

$$\sum_{i=1}^{n} \alpha_i . b_i \equiv S \; w \bmod M \; . \qquad \text{(III-81)}$$

Mas ,

$$\sum_{i=1}^{n} b_i < n.M$$

Seja $S' \equiv S \; w \bmod M$, tal que S' é o menor resíduo não negativo.

$$\sum_{i=1}^{n} \alpha_i . b_i \in \{ S', S'+M, \ldots, S'+(n-1)M \} \qquad \text{(III-82)}$$

O Método 1 é utilizado para determinar todas as soluções α para (III-82), e testar cada uma para verificar se é uma solução para (III-80). Se nenhuma solução for encontrada, então pode-se ter certeza de que não existem vetores binários α satisfazendo (III-80).

O desempenho do Método 2, analisado em [35], está intimamente relacionado com o desempenho do algoritmo L^3.

III.2.3.4.2.2 - MÉTODO DE LAGARIAS-ODLYZKO

Foi proposto por LAGARIAS e ODLYZKO [43] um algoritmo para determinar a solução do problema mochila. Este algoritmo, apesar de ser em tempo polinomial, nem sempre encontra uma solução, mesmo quando ela existe.

O método proposto constitui um ataque aos criptossistemas mochila de chave pública, sendo capaz de quebrá-los se eles transmitirem informação numa taxa inferior à densidade crítica.

O método de Lagarias-Odlyzko, denominado Algoritmo SV ("Short Vector"), é um método simples para localizar diretamente uma solução viável para o problema da mochila. O método consiste em transformar o problema mochila no problema de encontrar um vetor particular pequeno não-nulo γ em um reticulado inteiro e, então, aplicar o algoritmo L^3 de redução de base [50] para obter uma base reduzida do reticulado. Este método obtém sucesso se $\pm\gamma$ aparecer na base reduzida ; uma solução para o problema da mochila associado a este problema segue imediatamente de γ , como mostrado adiante.

A seguir são evidenciados os pontos básicos do algoritmo de Lagarias-Odlyzko.

==== MÉTODO DE ATAQUE ====

Suponha que é dado um vetor de inteiros positivos $a = (a_1, a_2, \ldots, a_n)$ e um inteiro S. O objetivo é encontrar, se existir, uma solução viável para :

$$\sum_{i=1}^{n} a_i \cdot x_i = S \qquad \text{(III-83)}$$

$$(x_i = 0 \text{ ou } 1 \quad \text{para} \quad i = 1, \ldots, n)$$

Basta considerar o caso em que $1 \leq S \leq \sum_{i=1}^{n} a_i$. Para determinar a solução de (III-83) será utilizado o algoritmo a seguir descrito.

ALGORITMO SV ("SHORT VECTOR")

Passo 1 : Tomar os seguintes vetores como uma base $[B_1, B_2, \ldots, B_{n+1}]^T$ para um reticulado inteiro $L = L(a,S)$ de dimensão n+1 :

$$\begin{aligned} B_1 &= (1, 0, \ldots, 0, -a_1) \\ B_2 &= (0, 1, \ldots, 0, -a_2) \\ &\vdots \\ B_n &= (0, 0, \ldots, 1, -a_n) \\ B_{n+1} &= (0, 0, \ldots, 0, S) \end{aligned} \qquad \text{(III-84)}$$

Passo 2 : Determinar uma base reduzida $[B_1^*, B_2^*, \ldots, B_{n+1}^*]$ de L usando o algoritmo L^3.

Passo 3 : Verificar se algum $B_i^* = (b_{i1}^*, b_{i2}^*, \ldots, b_{i,n+1}^*)$, não-nulo, tem todos os elementos

$b_{i,j}^* = 0$ ou λ , para algum λ inteiro fixo e $1 \leq j \leq n$

Para tal vetor B_i^* , verificar se $x_j = \lambda^{-1} . b_{i,j}^*$, para $1 \leq j \leq n$, fornece uma solução para o problema (III-83). Neste caso, pare o processamento. Caso contrário, continue.

Passo 4 : Repetir os Passos 1 a 3 com S sustituído por $S' = \sum_{i=1}^{n} a_i - S$. Então pare.

Se o Algoritmo SV determinar uma solução para (III-83), isto é,se for obtido o menor vetor não-nulo no reticulado L , diz-se que o algoritmo obteve sucesso, caso contrário, que falhou.

O desempenho do Algoritmo SV, que consiste essencialmente de duas aplicações do algoritmo L^3, depende fundamentalmente do desempenho do algoritmo de redução de base.

III.2.3.4.3 - ANÁLISE CRÍTICA

As duas técnicas de ataque ao criptossistema mochila de chave pública, descritas acima, empregam o algoritmo L^3 de redução de base de reticulado para determinar a solução para o problema mochila. Uma característica comum dessas técnicas é analisar a chave pública e o criptograma para determinar, diretamente, uma solução viável $x = (x_1, x_2, \ldots, x_n)$ para a mensagem (texto claro).

O método de BRICKELL [35] é usado para resolver problemas mochila que apresentam densidade menor que $1/\log_2 n$. No caso de mochilas mais densas, pode-se tentar diminuir, artificialmente, a densidade da mochila, aplicando-se uma transformação modular $w \bmod M$ com parâmetros adequadamente escolhidos, para, então, poder aplicar o método proposto. No entanto, isso nem sempre funciona, obtendo-se sucesso somente sob certas condições, o que restringe o emprego do algoritmo. Uma vantagem importante do ataque proposto por Brickell é a sua utilização tanto em problemas mochila de iteração simples como em mochilas de iteração múltipla.

O método de LAGARIAS-ODLYZKO [43], denominado Algoritmo SV ("Short Vector"), funciona para mochilas de baixa densidade, como segue :

- Existe uma densidade crítica, d_c, abaixo da qual o algoritmo de Lagarias-Odlyzko funciona para "quase todos" os problemas mochila de densidade $d(a) < d_c$, e para $d(a) \geq d_c$ o algoritmo "quase nunca" funciona. Testes realizados sugeriram que $d_c = 0{,}645\ldots$
- "Quase todos" os problemas mochila com $d(a) < 0{,}645$ podem ser resolvidos em tempo polinomial usando o Algoritmo SV que "quase sempre" determina o vetor não-nulo de menor norma Euclideana no reticulado inteiro $L = L(a,S)$, sendo $\sum_{i=1}^{n} x_i . a_i = S$, $x_i = 0$ ou 1 para $1 \leq i \leq n$.

- Para "quase todos" os problemas mochila solúveis com n elementos , tendo $d(a) < (2-\varepsilon)/n \cdot \log_2 4/3$, para algum $\varepsilon > 0$ fixo , o Algoritmo SV encontra a solução.
- Pode-se esperar que o Algoritmo SV resolva até mesmo problemas mochila relativamente densos.

Na análise apresentada em [43] é mostrado que o desempenho do Algoritmo SV só não é melhor devido ao algoritmo de redução de base, que nem sempre produz o menor vetor não-nulo no reticulado inteiro L .

Lagarias-Odlyzko executaram testes computacionais exaustivos usando o algoritmo SV para avaliar seu desempenho. Foram testadas diversas variantes do algoritmo SV, obtidas a partir de modificações no Algoritmo L^3, introduzidas a fim de aumentar a sua chance de encontrar o menor vetor não-nulo num reticulado. Duas modificações principais foram consideradas. Os resultados obtidos, assim como a análise do desempenho do algoritmo, são apresentadas em [43].

Um outro autor, A.M.FRIEZE [51], desenvolveu uma análise do algoritmo de Lagarias-Odlyzko para quebrar o criptossistema mochila de chave pública. O objetivo principal deste artigo foi fornecer uma prova simples do resultado do algoritmo de Lagarias-Odlyzko.

Testes aplicados aos criptossistemas mochila de chave pública indicaram que o método de Lagarias-Odlyzko pode ser aplicado não só a mochilas de iteração simples, mas também a mochilas de iteração múltipla. O método também pode ser empregado para resolver problemas mochila mais densos. Para isso basta converter o problema em um outro de baixa densidade, utilizando-se uma ou mais multiplicações modulares. Espera-se que tais multiplicações ajudem a resolver o problema original após a aplicação do Algoritmo SV . (Esta sugestão também foi feita por BRICKELL [35]).

Comparando-se o Método de Brickell com o de Lagarias-Odlyzko, observa-se que são similares, porém o primeiro apresenta vantagens práticas sobre este último devido ao processamento inicial executado que garante o "quase sucesso" nos passos seguintes do algoritmo. Outra observação é que a densidade crítica abaixo da qual o método de Brickell funciona (0,44) é menor que para o Algoritmo SV (0,645). O desempenho de ambos os métodos descritos está intimamente relacionado com o desempenho do algoritmo L^3 de redução de base.

Como os métodos de ataque apresentam melhor resultado quando aplicados a mochilas de baixa densidade, para se ter um sistema seguro do ponto de vista criptoanalítico, o mesmo deve ser projetado de forma a apresentar alta densidade.

Com base no que foi mostrado sobre os métodos para quebrar criptossistemas mochila de chave pública, pode-se concluir que :

- Evidências empíricas indicam que os métodos muito provavelmente quebrarão todos os criptossistemas mochila para os quais $d(a) < d_c$, em tempo polinomial. Em particular, também quebrarão "quase todos" os criptossistemas de SHAMIR [32], já que estes apresentam $d(a) < 1/\log_2 n$.

- Estes métodos complementam aqueles ataques a criptossistemas mochila que são baseados na recuperação da informação "trapdoor". Quando a taxa de informação for baixa, os métodos de Brickell e de Lagarias-Odlyzko devem funcionar. Para os casos em que a expansão de dados é baixa (o que corresponde ao sistema ter alta densidade), torna-se mais difícil esconder a informação "trapdoor" e, portanto, ataques baseados em determiná-la terão maior probabilidade de sucesso.

CAPÍTULO IV

NOVAS FORMULAÇÕES PARA CRIPTOSSISTEMAS MOCHILA DE CHAVE PÚBLICA

IV.1 - CONSIDERAÇÕES INICIAIS

Atualmente existe um grande interesse no problema de se conseguir comunicação segura de mensagens digitais em canais de comunicação expostos publicamente, com o propósito de esconder, dos receptores não autorizados, o conteúdo das mensagens transmitidas. Ocorre comunicação segura, entre dois indivíduos, quando eles se comunicam privadamente, a despeito dos esforços de uma terceira pessoa (o interceptador) para entender o que está sendo comunicado.

Durante anos, o criptossistema de chave pública, mais especificamente o sistema criptográfico tipo mochila de MERKLE e HELLMAN [3], foi considerado como um esquema atrativo para proteger a transmissão de informações contra os interceptadores. No entanto, o sistema de Merkle e Hellman possui algumas fraquezas criptoanalíticas, evidenciadas pelos métodos de ataque apresentados no capítulo anterior.

O aparecimento dos primeiros métodos de criptoanálise do sistema mochila de chave pública deu início a maiores pesquisas nesta área e, em decorrência, muitos novos esquemas têm sido propostos para proteger a privança das mensagens. Por isso, com o propósito de obter um criptossistema mochila mais seguro que o sistema original proposto por Merkle e Hellman, muitos pesquisadores têm sugerido novas formulações para o sistema mochila de chave pública.

O enfoque mais empregado por vários autores é tentar evitar as técnicas de quebra utilizando modificações no algoritmo original de Merkle e Hellman. Uma outra maneira é utilizar uma formulação completamente diferente. Todas estas tentativas de novas formulações visam a obter um algoritmo de chave pública que resista a alguns (se não a todos) ataques criptoanalíticos conhecidos.

IV.2 - CLASSIFICAÇÃO DAS FORMULAÇÕES

Muitos pesquisadores têm se preocupado com a segurança criptográfica do SCMH, e têm apresentado sugestões para torná-lo mais seguro. Novas formulações podem ser encontradas na literatura, nas quais as modificações propostas para o método original visam a obter algum algoritmo tipo mochila mais resistente às investidas criptoanalíticas.

Neste capítulo serão apresentadas algumas generalizações, ou novas formulações, para o sistema criptográfico de chave pública tipo mochila, ressaltando-se os pontos relevantes de cada algoritmo, numa abordagem crítica.

A leitura de vários artigos, encontrados na literatura sobre o assunto, permitiu identificar as características básicas de cada formulação, possibilitando, por conseguinte, estabelecer uma taxonomia dos diferentes enfoques ao criptossistema mochila.

As diferentes formulações podem ser classificadas, segundo a idéia básica de seu algoritmo, nos seguintes grupos:

1º - Sistema usando chave secreta supercrescente

Formulação muito parecida com o algoritmo original de Merkle-Hellman, com algumas mudanças. Neste grupo se encontram os sistemas que utilizam seqüência k-supercrescente e matriz de difusão, sistemas com ruído deliberado, e sistemas de soma aleatória (mochila aditiva).

2º - Sistema usando chave secreta não-supercrescente

É diferente do caso anterior pois, apesar de manter a mesma estrutura básica nos algoritmos, utiliza, para gerar a chave pública, mochila não supercrescente, que pode ser : mochi

la "útil", mochila "fácil", mochila arbitrária qualquer, ou ainda utilizar transformações modulares não M-dominantes com incorporação de ruído.

3º - Sistema utilizando Números Primos

Neste caso a segurança do sistema criptográfico reside, também, na dificuldade de fatoração de primos. As formulações utilizam os conceitos de inverso multiplicativo, multiplicador matricial, representações modular e radial, e elementos idempotentes.

4º - Sistema considerando Corpos Finitos

Compreende os sistemas que usam recursos da Álgebra de Corpos Finitos: sistemas utilizando polinômios irredutíveis, logaritmos discretos, e Códigos de Correção de Erro.

A descrição detalhada de cada sistema é apresentada nos itens subsequentes.

IV.2.1 - CHAVE SECRETA SUPERCRESCENTE

IV.2.1.1 - SEQÜÊNCIA k-SUPERCRESCENTE E MATRIZ DE DIFUSÃO

Sejam $k = (k_1, k_2, \ldots, k_n)$ e $a = (a_1, a_2, \ldots, a_n)$ duas seqüências de números naturais positivos não nulos.

Uma seqüência $a = (a_1, a_2, \ldots, a_n)$ é dita k-supercrescente se, e somente se :

$$a_j > \sum_{i=1}^{j-1} k_i . a_i \quad , \quad j = 2, \ldots, n$$

$$a_1 > 0 \ , \text{ qualquer}$$

A seqüência k-supercrescente é também chamada de "seqüência supercrescente generalizada".

Observa-se que a definição de seqüência supercrescente utilizada por MERKLE e HELLMAN [3] é um caso particular da seqüência supercrescente generalizada, onde $k = (k_1, k_2, \ldots, k_n)$ é tal que $k_i = 1$ para $i = 1, \ldots, n$.

PAZ DE LIMA [46] e RETKIN [39] propuseram, independentemente, uma generalização para o criptossistema mochila de chave pública, empregando, basicamente, uma chave secreta k-supercrescente e uma matriz de difusão para obtenção da chave pública de cifrar.

A seguir é apresentada a conceituação básica de cada formulação.

IV.2.1.1.1 - CONCEITUAÇÃO BÁSICA

IV.2.1.1.1.1 - FORMULAÇÃO DE RETKIN

Em sua formulação RETKIN [39] propôs a utilização de um vetor chave secreta $a' = (a'_1,\ldots,a'_n)$ satisfazendo a seguinte restrição :

$$a'_j > \sum_{i=1}^{j-1} k_i . a'_i \quad , \quad j = 2,3,\ldots,n \qquad (IV-1)$$

$$a'_1 > 0 \ , \text{ qualquer}$$

para algum vetor inteiro $k = (k_1,\ldots,k_n)$.

A formulação inicial do autor, embora não apresentada desta forma, equivale a considerar o vetor $k = (k_1,\ldots,k_n)$ com todos os elementos iguais entre si. Na formulação modificada os elementos deste vetor podem ter valores diferentes. Para ambas as formulações, no entanto, a obtenção da chave pública e os processos de cifração e decifração são idênticos.

Seja $x = (x_1,\ldots,x_n)$ um vetor de inteiros que representa a mensagem, tal que :

$$0 \leq x_i \leq k_i \quad , \quad i = 1,2,\ldots,n \qquad (IV-2)$$

e seja $a' = (a'_1,\ldots,a'_n)$ um vetor-linha de tamanho n, cujos elementos formam uma seqüência k-supercrescente. Então, para o número inteiro S' , dado por :

$$S' = x \, . \, (a')^T \qquad (IV-3)$$

o vetor mensagem $x = (x_1,\ldots,x_n)$ pode ser determinado, sem dificuldade, aplicando-se o Teorema Fundamental da Divisão.

O vetor $a' = (a'_1,...,a'_n)$ pode ser substituído pela "forma disfarçada" $a = (a_1,...,a_n)$, do seguinte modo :

$$a_i \equiv w \cdot a'_i \mod M \quad , \quad i = 1,...,n$$
$$a'_i \equiv w^{-1} \cdot a_i \mod M \quad , \quad i = 1,...,n \qquad \text{(IV-4)}$$

onde w e M são inteiros tais que :

$$(w,M) = 1$$
$$0 < w < M \qquad \text{(IV-5)}$$

Utilizando-se o vetor $a = (a_1,...,a_n)$, a cifração de um vetor-mensagem não-binário torna-se possível.

O uso de vetores-mensagem não-binários significa que vetores menores podem manipular um dado dicionário de mensagens, o que implica que vetores-mochila menores podem ser usados sem, no entanto, afetarem a dificuldade de um ataque criptoanalítico.

Explorando as vantagens de um sistema criptográfico tipo mochila k-supercrescente, Retkin utilizou o conceito de matriz de difusão, definida como uma matriz não-singular (admite inversa) cujos elementos são inteiros não-negativos, e tem a propriedade de que a soma dos elementos da i-ésima coluna é menor ou igual ao inteiro k_i (isto é, o valor k_i é o valor limite para a soma dos elementos da i-ésima coluna da matriz de difusão D).

Segundo RETKIN [39], a segurança do criptossistema mochila pode ser substancialmente melhorada pelo uso da matriz de difusão como uma chave adicional.

Sejam $p = (p_1,...,p_n)$ um vetor-mensagem binário, e D uma matriz de difusão em que cada coluna i apresenta a soma de seus elementos menor ou igual a k_i (para garantir decifração única), então :

$$x = p \cdot D \qquad \text{(IV-6)}$$

é um vetor-mensagem não-binário que pode ser cifrado como o número S calculando-se :

$$S = x \cdot a^T = p \cdot D \cdot a^T \qquad \text{(IV-7)}$$

onde D é uma matriz de dimensão (n x n) .

Para decifrar a mensagem, o valor S é primeiramente substituído por :

$$S' = w^{-1} \cdot S \bmod M \qquad \text{(IV-8)}$$

De posse do valor S' pode-se, então, determinar :

$$S' = w^{-1} \cdot p \cdot D \cdot a^T \bmod M$$

$$S' = p \cdot D \cdot (a')^T \qquad \text{(IV-9)}$$

e sendo $a' = (a'_1,...,a'_n)$ uma seqüência k-supercrescente, o vetor-mensagem não-binário $x = (x_1,...,x_n) = p \cdot D$ pode ser recuperado utilizando-se o Teorema Fundamental da Divisão (como apresentado no exemplo a seguir). Finalmente, o vetor-mensagem binário pode ser obtido usando-se a inversa da matriz D :

$$p = x \cdot D^{-1} \qquad \text{(IV-10)}$$

A mochila secreta $a' = (a'_1,...,a'_n)$ é construída de modo a ser k-supercrescente, e é transformada para a forma disfarçada $a = (a_1,...,a_n)$ segundo (IV-4). A este vetor é aplicada a matriz de difusão para torná-lo um vetor-linha $u = (u_1,...,u_n)$ dado por :

$$u = a \cdot D^T \qquad \text{(IV-11)}$$

e este é o vetor que será publicado como o vetor de cifrar, usado na cifração da seqüência binária $p = (p_1,...,p_n)$ que representa a mensagem em texto claro. Isto é, $u = (u_1,...,u_n)$, ou uma permutação deste vetor, é a chave pública disponível para o usuário.

A implementação de um sistema criptográfico tipo mochila k-supercrescente com difusão envolve, primeiramente, a construção da forma inicial do vetor-mochila secreto (após decidir sobre os valores dos elementos do vetor $k = (k_1,..., k_n)$) , transformando, depois, na forma disfarçada correspondente (usando multiplicação modular) , e finalmente multiplicando este último vetor pela matriz de difusão adequada. O resultado final deste processo é o vetor-mochila público, o qual é usado para converter vetores-mensagem binários em números reais.

No caso especial em que $k = (1,1,...,1)$, o único tipo de matriz de difusão disponível é a matriz obtida pela permutação das linhas da matriz identidade. Isso simplesmente tem o efeito de permutar os elementos dentro da seqüência mochila $a = (a_1,...,a_n)$.

A fim de estabelecer uma mochila k-supercrescente para um criptossistema de chave pública, é mais conveniente decidir primeiro sobre a matriz de difusão, na qual a soma de cada coluna não é maior que os valores k_i que serão usados para formar a seqüência k-supercrescente. Em [39] são apresentadas algumas maneiras de se obter matriz de difusão adequada para ser usada no sistema criptográfico descrito acima.

IV.2.1.1.1.2 - FORMULAÇÃO DE PAZ DE LIMA

A formulação de PAZ DE LIMA [46] é similar àquela formulação de RETKIN [39] em que o vetor $k = (k_1,\ldots,k_m)$ possui seus elementos diferentes entre si.

De acordo com [46], o vetor $k = (k_1,\ldots,k_m)$ deve ser obtido a partir de uma matriz D, que é mantida secreta, escolhida de modo que exista a matriz inversa D^{-1} . Esta matriz não precisa ser quadrada, basta que tenha inversa á direita.

Seja :

$$D = \begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1m} \\ d_{21} & d_{22} & \cdots & d_{2m} \\ \vdots & & & \\ d_{n1} & d_{n2} & \cdots & d_{nm} \end{bmatrix} \qquad \text{(IV-12)}$$

onde : D é a matriz de transformação ou de difusão, de dimensão (n x m), com $m \geq n$, e existe a matriz D_d^{-1} (matriz inversa à direita) ;

$\sum_{i=1}^{n} d_{ij}$ é a soma dos elementos da j-ésima coluna da matriz D .

Assim o vetor $k = (k_1,\ldots,k_m)$ será :

$$k = (k_j)_{j=1,m}$$

$$k_j \geq \sum_{i=1}^{n} d_{ij} \quad , \quad j = 1,\ldots,m \qquad \text{(IV-13)}$$

Uma vez construído o vetor $k = (k_1,...,k_m)$, obtém-se facilmente a seqüência k-supercrescente, utilizando-se a relação :

$$a'_j > \sum_{i=1}^{j-1} k_i . a'_i \quad , \quad j = 2,3,...,m \qquad (IV-14)$$

$$a'_1 > 0 \ , \text{ qualquer}$$

A seqüência k-supercrescente e a matriz D são mantidas secretas.

A chave pública, seqüência $a = (a_1,...,a_n)$, é obtida fazendo-se a multiplicação da matriz de difusão D pela seqüência secreta k-supercrescente :

$$a^T = D . (a')^T \qquad (IV-15)$$

onde : D é a matriz de difusão (n x m) ;

$a' = (a'_1,...,a'_m)$ é o vetor k-supercrescente (1 x m);

$a = (a_1,...,a_n)$ é o vetor chave pública (1 x n);

T é o índice que significa "transposto"

O vetor $a = (a_1,...,a_n)$ assim obtido não é, em geral, supercrescente.

O criptograma S ,a ser enviado ao receptor autorizado, é obtido como no SCMH, calculando-se o produto escalar entre o vetor-mensagem binário $x = (x_1,...,x_n)$ e a chave pública de cifrar $a = (a_1,...,a_n)$:

$$S = x . a^T \qquad (IV-16)$$

Usando a equação (IV-15) pode-se escrever :

$$S = x . D . (a')^T \qquad (IV-17)$$

$$S = (x . D) . (a')^T$$

Uma vez que o vetor $a' = (a'_1 ,...,a'_m)$ é k-supercrescente, obtém-se, a partir de S e usando o Teorema Fundamental da Divisão (veja exemplo a seguir), o vetor-mensagem não-binário $x' = (x'_1 ,...,x'_m)$:

$$x' = x \cdot D \qquad \text{(IV-18)}$$

e daí, então, recupera-se o vetor-mensagem $x = (x_1,...,x_n)$, que é a seqüência binária que representa o texto claro :

$$x = x' \cdot D_d^{-1} = x \cdot D \cdot D_d^{-1} \qquad \text{(IV-19)}$$

A essência da formulação de Paz de Lima é utilizar uma matriz D ,invertível à direita, e uma seqüência supercrescente generalizada $a' = (a'_1 ,..., a'_m)$ para obter a chave de cifrar $a = (a_1 ,..., a_n)$, conforme (IV-15).

IV.2.1.1.2 - EXEMPLO DE APLICAÇÃO

Seja a matriz D escolhida tal que exista D_d^{-1} :

$$D = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \qquad \therefore \qquad D_d^{-1} = \begin{bmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ -1 & 1 & 1 \end{bmatrix}$$

$$\sum_{i=1}^{3} d_{i1} = 1 + 0 + 1 = 2$$

$$\sum_{i=1}^{3} d_{i2} = 1 + 1 + 0 = 2$$

$$\sum_{i=1}^{3} d_{i3} = 1 + 1 + 1 = 3$$

Seja escolhido o vetor k = (2, 2, 3).

A partir do vetor k obtém-se a seqüência k-supercrescente (chave secreta) :

$a'_1 = 4$ (valor arbitrário)

$a'_2 > k_1 . a'_1 = 2 \times 4 = 8 \qquad \therefore \qquad a'_2 = 10$

$a'_3 > k_1 . a'_1 + k_2 . a'_2 = 8 + 20 = 28 \qquad \therefore \qquad a'_3 = 30$

a' = (4, 10, 30) é (2,2,3)-supercrescente .

A chave pública é obtida da seguinte forma :

$$a^T = D \,.\, (a')^T = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} . \begin{bmatrix} 4 \\ 10 \\ 30 \end{bmatrix}$$

a = (44, 40, 34)

Este vetor é utilizado para cifrar as mensagens binárias.

Para o bloco de mensagem $x = (1, 1, 0)$, o criptograma será :

$$S = x \cdot a^T = (1, 1, 0) \cdot (44, 40, 34)^T$$

$$S = 84$$

O receptor, de posse do valor S, determina o vetor $x' = (x'_1, x'_2, x'_3)$ da seguinte forma :

$$S = x \cdot D \cdot (a')^T = x' \cdot (a')^T$$

$$84 = x' \cdot (a')^T$$

Como o vetor $a' = (4, 10, 30)$ é $(2,2,3)$-supercrescente, pode-se utilizar o Teorema Fundamental da Divisão para determinar o vetor $x' = (x'_1, x'_2, x'_3)$ a partir de $S = 84$. Este Teorema estabelece que :

"Dados dois inteiros P e p, $p > 0$, existe um único par de inteiros q e r tal que :

$$P = p.q + r \quad , \quad 0 \leq r < p. "$$

Assim vem :

$$S = 84 = x'_3 \cdot a'_3 + r_3 = 30.x'_3 + r_3$$

Como é necessário que $r_3 < 30$, então: $x'_3 = 2$

$$r_3 = 84 - 2 \times 30 = 24$$

$$24 = x'_2 \cdot a'_2 + r_2 = 10.x'_2 + r_2$$

Para $r_2 < 10$, tem-se : $x'_2 = 2$

$$r_2 = 24 - 2 \times 10 = 4$$

$$4 = x'_1 \cdot a'_1 = 4.x'_1 \quad \therefore \quad x'_1 = 1$$

Portanto :

$$x' = (1, 2, 2)$$

A partir do vetor x' obtém-se o vetor-mensagem binário x, aplicando a multiplicação matricial :

$$x = x' \cdot D_d^{-1}$$

$$x = (1, 2, 2) \cdot \begin{bmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ -1 & 1 & 1 \end{bmatrix}$$

$$x = (1, 1, 0)$$

Desta forma o receptor autorizado conseguiu recuperar, com facilidade, o texto claro correspondente ao criptograma recebido.

IV.2.1.1.3 - COMENTÁRIOS

O método proposto por RETKIN [39] apresenta, em sua formulação, as mesmas características básicas do método original proposto por MERKLE e HELLMAN [3], e permite cifrar e decifrar mensagens não-binárias. O uso de vetores-mensagem não binários significa que vetores menores podem manipular um dado dicionário de mensagens, o que implica que vetores-mochila menores podem ser usados sem, no entanto, afetarem essencialmente a dificuldade de um ataque criptoanalítico.

Uma vez que não existe nenhuma grande vantagem no uso da versão não-binária do SCMH, Retkin utilizou o conceito de matriz de difusão para aumentar, substancialmente, a segurança do método. Esta matriz, considerada como uma chave adicional, é empregada na obtenção da chave pública de cifrar.

A essência da formulação de PAZ DE LIMA [46] é a utilização de uma matriz de difusão invertível (que pode ser retangular), e de uma seqüência supercrescente generalizada, para obter a chave de cifrar (o vetor público), sem empregar a transformação modular w.mod M . Neste caso a matriz de difusão pode ser considerada como um multiplicador matricial da seqüência supercrescente.

A vantagem da formulação de Paz de Lima é que a matriz de difusão pode ser retangular, implicando que as chaves de cifrar e de decifrar tenham tamanhos diferentes, e, desta forma nega informação ao adversário.

O método de Paz de Lima se aplica para mensagens binárias, podendo, no entanto, ser generalizado para mensagens não-binárias.

A utilização de seqüências k-supercrescentes, nas formulações apresentadas em [39] e [46], caracteriza uma fraqueza criptográfica que pode ser explorada pelos criptoanalistas. Mas, por outro lado, a utilização da matriz de difusão compensa esta fraqueza.

A multiplicação matricial (matriz D), em substituição ao multiplicador escalar (valor w) do Sistema Merkle-Hellman, usada como forma de esconder a propriedade de supercrescimento, evita as criptoanálises que dependem do fato de o multiplicador ser o mesmo para todos os elementos da chave secreta, isto é, evita os ataques de recuperação da informação "trapdoor" [25], [27] e [29].

A construção dos métodos de Retkin e de Paz de Lima , porém, não garante resistência aos ataques criptoanalíticos por reduções sucessivas [6], [21] e [26], nem aos ataques a mochilas de baixa densidade [35] e [43].

IV.2.1.2 - SISTEMA COM RUÍDO DELIBERADO

Em geral, os métodos de criptoanálise são projetados para descobrir uma fraqueza estrutural ou uma fraqueza estatística no algoritmo criptográfico.

Uma fraqueza estrutural pode ser causada, por exemplo, pela escolha inadequada dos parâmetros "trapdoor" do esquema de chave pública. Já os testes de fraqueza estatística são projetados para fazer inferências sobre a função de decifrar desconhecida, examinando-se (se possível) os criptogramas de saída, ou um conjunto de pares texto claro/criptograma conhecidos. Considera-se, usualmente, que o criptoanalista conhece algumas estatísticas da fonte do texto claro, isto é, conhece, por exemplo, as freqüências das letras, dos bigramas,etc, do idioma.

Em 1980 WILLETT [10] apresentou métodos para incorporar ruído deliberado (ou erros), pelo elemento que cifra a mensagem, em criptossistemas clássico e de chave pública, a fim de confundir o uso de estatísticas da fonte conhecidas pelo criptoanalista e, assim, aumentar a segurança dos sistemas criptográficos.

O ruído deve ser introduzido no processo de cifração de modo que o receptor autorizado possa removê-lo, mas, por outro lado, esta remoção pelo interceptador seja, pelo menos, tão difícil quanto quebrar o esquema criptográfico original, isto é, sem ruído.

Como aplicação do esquema de chave pública contendo ruído intrínseco (ruído introduzido antes do processo de cifração), WILLETT [10] considerou uma modificação no SCMH, apresentada a seguir.

IV.2.1.2.1 - CONCEITUAÇÃO BÁSICA

Considerando a propriedade de supercrescimento da mochila $a' = (a'_1 , \ldots , a'_n)$, WILLETT [10] introduziu o conceito de "distância mínima" da mochila.

Para um vetor supercrescente $a' = (a'_1 , \ldots , a'_n)$ dado e a função $f_{a'}(x) = a' \cdot x^T$, com $x = (x_1 , \ldots , x_n)$ sendo uma n-pla binária, seja :

$$d(a') = \min_{x \neq y} \left| f_{a'}(x) - f_{a'}(y) \right| \qquad \text{(IV-20)}$$

a distância mínima entre dois pontos no conjunto de valores da função $f_{a'}$.

A distância mínima de um vetor supercrescente definido por $a' = (a'_1 , \ldots , a'_n)$ é facilmente computada [10] da seguinte forma :

$$d(a') = \min \left\{ \{a'_1\} \cup \{a'_j - \sum_{i=1}^{j-1} a'_i \mid 2 \leq j \leq n \} \right\} \qquad \text{(IV-21)}$$

Seja :

$$e(a') = \frac{(d(a') - 1)}{2} \qquad \text{(IV-22)}$$

Se $f_{a'}(x) = S'$ e $\bar{S}' = S' + r'$, onde $|r'| \leq e(a')$, então $\bar{S}'$ é ainda mais próximo de S' que qualquer outro valor no conjunto de valores de função $f_{a'}$.

Desta forma, se r' for usado deliberadamente como ruído no esquema de cifração, considerando a mochila supercrescente $a' = (a'_1 , \ldots , a'_n)$ como chave de cifrar, então a mensagem $x = (x_1 , \ldots , x_n)$ pode ser recuperada a partir de $\bar{S}'$ se o ruído deliberado r' satisfizer a condição $|r'| \leq e(a')$, empregando-se o seguinte algoritmo :

- ALGORITMO PARA MOCHILA SUPERCRESCENTE COM RUÍDO: $|r'| \leq e(a')$

INÍCIO

PARA $i = n, n-1, \ldots, 1$ FAÇA

SE

$$\left\{ \bar{S}' - \sum_{j=i+1}^{n} a'_j . x_j \right\} \geq a'_i - e(a')$$

(O somatório é zero para $i = n$)

ENTÃO $x_i = 1$

SENÃO $x_i = 0$

FIM

Para um sistema criptográfico seguro, no entanto, a chave de cifrar não pode ser supercrescente e, por isso, a mochila $a' = (a'_1 , \ldots , a'_n)$ é convertida na mochila pública $a = (a_1 , \ldots , a_n)$ usando uma transformação modular $w \bmod M$, conforme (IV-4) e onde w e M satisfazem (IV-5). Neste caso, os valores permitidos para o ruído são diferentes.

Considerando a mochila pública $a = (a_1 , \ldots , a_n)$, o criptograma a ser enviado ao receptor autorizado será :

$$\bar{S} = (a \, . \, x^T) + r = S + r \qquad \text{(IV-23)}$$

onde : $x = (x_1 , \ldots , x_n)$ é o vetor-mensagem binário ;

$a = (a_1 , \ldots , a_n)$ é a chave de cifrar ;

r é o ruído utilizado.

A fim de que o vetor $x = (x_1 , \ldots , x_n)$ possa ainda ser recuperado a partir de :

$$\bar{S}' = w^{-1} \, . \, (S + r) \bmod M \qquad \text{(IV-24)}$$

usando o algoritmo acima, é claro que a condição

$$| \, w^{-1} . \, r \bmod M \, | \leq e(a') \qquad \text{(IV-25)}$$

tem que ser satisfeita, o que requer que r seja escolhido de um conjunto R ,

$$R = \{ r' \cdot w \bmod M \mid |r'| \leq e(a') \} \qquad \text{(IV-26)}$$

Como parte da informação pública pode-se fornecer um subconjunto de R como sendo o conjunto de ruídos permitidos.

O usuário que vai transmitir a mensagem calcula :

$$S = a \cdot x^T \qquad \text{(IV-27)}$$

e então escolhe aleatoriamente o ruído r do conjunto de ruídos permitidos, e transmite o criptograma $\bar{S}$, calculado conforme a expressão (IV-23).

O receptor, de posse do valor $\bar{S}$, efetua a multiplicação modular inversa para obter $\bar{S}'$ usando a expressão (IV-24).

Uma vez obtido o valor de $\bar{S}'$ e conhecidos os valores permitidos para o ruído r (definidos por um subconjunto de R), emprega-se o algoritmo para mochila supercrescente apresentado acima e, então, recupera-se o vetor-mensagem $x = (x_1, \ldots, x_n)$ facilmente. (É claro que o algoritmo só pode ser usado se a condição (IV-25) para r tiver sido satisfeita.)

Seja $\{ r_1, r_2, \ldots, r_k \} \subseteq R$ um conjunto de valores de ruído revelados publicamente. O criptoanalista se depara com o fato de resolver um problema mochila modificado :

$$(a_1, \ldots, a_n, r_1, \ldots, r_k) \cdot (x_1, \ldots, x_n, y_1, \ldots, y_k)^T = \bar{S} \qquad \text{(IV-28)}$$

onde $y_i \in \{ 0,1 \}$, $i = 1, \ldots, k$ e, no máximo, um dos elementos y_i é 1(um). Este problema é equivalente a resolver o problema mochila aumentado.

IV.2.1.2.2 - EXEMPLO DE APLICAÇÃO

Para um sistema mochila binário, seja considerado o seguinte vetor supercrescente :

$$a' = (6, 11, 23, 47)$$

A distância mínima para este vetor é :

$$d(a') = \min \left\{ \{6\} \cup \{(11-6),(23-17),(47-40)\} \right\}$$

$$d(a') = 5$$

Assim : $e(a') = \frac{5 - 1}{2} = 2$

$$|r'| \leq 2$$

Sejam ainda : $M = 101$

$w = 23 \quad \therefore \quad w^{-1} = 22 \bmod 101$

Calculando-se a chave pública obtém-se :

$$a_i = a'_i \cdot w \bmod M \quad , \quad i = 1,2,3,4$$

$$a = (37, 51, 24, 71)$$

Um conjunto de ruídos permitidos para este caso será :

$$R = \{ r' \cdot w \bmod M \mid |r'| \leq 2 \}$$

$r' = 1 \rightarrow r = 1x23 \bmod 101 = 23$
$r' = 2 \rightarrow r = 2x23 \bmod 101 = 46$
$r' = -1 \rightarrow r = (-1)x23 \bmod 101 = -23 = 78$
$r' = -2 \rightarrow r = (-2)x23 \bmod 101 = -46 = 55$

$$R = \{ 23, 46, -23, -46, 78, 55 \}$$

Seja a mensagem binária : $x = (1, 0, 1, 1)$

Escolhendo $r = -46$ o criptograma será :

$$\bar{S} = (a.x^{T}) + r$$

$$\bar{S} = (37 + 24 + 71) + (-46) \quad \therefore \quad \bar{S} = 86$$

Para decifrar a mensagem o receptor calcula :

$$\bar{S}' = w^{-1} . \bar{S} \bmod M$$

$$\bar{S}' = 22 \times 86 \bmod 101 \quad \therefore \quad \bar{S}' = 74$$

E executa o algoritmo :

$i = 4$, $(74) > (47-2=45) \rightarrow x_4 = 1$

$i = 3$, $(74-47=27) > (23-2=21) \rightarrow x_3 = 1$

$i = 2$, $(74-70= 4) < (11-2=9) \rightarrow x_2 = 0$

$i = 1$, $(74-70= 4) = (6-2=4) \rightarrow x_1 = 1$

E assim a mensagem é recuperada:

$$x = (1, 0, 1, 1)$$

IV.2.1.2.3 - COMENTÁRIOS

O método proposto por WILLETT [10], para incorporar ruído deliberado em criptossistemas mochila de chave pública, tem a finalidade de gerar homofonia pela escolha aleatória do elemento y_i que será considerado igual a 1(um) na expressão (IV-28). O ruído introduz um elemento de aleatoriedade, disfarçando as estatísticas originais da fonte no bloco da cifra, e desta forma, dificulta ataques estatísticos. Mas, por outro lado, revelando um subconjunto de valores permitidos para o ruído, o usuário pode introduzir uma fraqueza estrutural no sentido de que o criptoanalista estará em uma posição melhor para determinar as incógnitas w e M .

Quanto à segurança criptográfica do método proposto por WILLETT [10] pode-se observar que este esquema é vulnerável aos ataques de recuperação da informação "trapdoor" [25], [27] e [29], pelo fato de usar seqüência supercrescente como chave secreta e empregar transformação modular M-dominante.

Este esquema não garante resistência aos ataques criptoanalíticos por reduções sucessivas [6], [21] e [26], e nem aos ataques a mochilas de baixa densidade [35] e [43], pois não foi formulado com este propósito.

Uma sugestão desta tese, para melhorar o método de ruído deliberado, no sentido de torná-lo um pouco mais seguro às investidas criptoanalíticas, é a formulação de um esquema similar ao de WILLETT[10], com matriz de difusão e seqüência k-supercrescente como chave secreta, conforme apresentado nas formulações de RETKIN [39] e de PAZ DE LIMA [46]. A matriz de difusão, usada como chave adicional, introduzirá um fator complicador na criptoanálise, e então o método terá condição de resistir aos ataques de recuperação da informação "trapdoor". Os valores de ruído serão transformados também pela matriz de difusão (e não só pelos parâmetros w e M), e, desta forma, a publicação de valores permitidos para o ruído não comprometerá a segurança do sistema como um todo.

IV.2.1.3 - SISTEMA DE SOMA ALEATÓRIA (MOCHILA ADITIVA)

Em situações práticas, normalmente, se deseja cifrar uma mensagem específica diferentemente cada vez que ela é transmitida. Geralmente, isso é feito acrescentando-se, à mensagem binária, um sufixo binário aleatório e cifrando a mensagem completa formada por esta combinação. Desta forma, se uma mensagem binária de h bits precisar ser criptografada de 2^n maneiras diferentes, usando o SCMH, o sufixo aleatório será de tamanho n bits, e o vetor público (chave de cifrar) deverá conter h+n elementos.

Em 1980 ARAZI [12] sugeriu um criptossistema de chave pública para cifrar uma mensagem, de valor numérico limitado por M , de 2^n modos distintos usando uma mochila de n elementos. Isso é feito adicionando-se ao valor numérico da mensagem a soma de um número qualquer de elementos selecionados aleatoriamente da mochila pública, permitindo, assim, representação múltipla da mensagem. (Valor numérico da mensagem é o valor decimal correspondente à representação binária da mensagem.)

As características da formulação de Arazi são apresentadas a seguir.

IV.2.1.3.1 - CONCEITUAÇÃO BÁSICA

No sistema criptográfico proposto por ARAZI [12], seja $a' = (a'_1 , \ldots , a'_n)$ uma seqüência supercrescente onde cada elemento a'_i é escolhido aleatoriamente de uma distribuição uniforme no intervalo :

$$[(2^i - 1).2^h + 1 \; ; \; 2^{h+i}] \qquad i = 1,2,\ldots,n$$

para um inteiro positivo h .

Seja ainda o inteiro m escolhido do intervalo :

$$[2^{n+h+2} + 1 \; ; \; 2^{n+h+3} - 1] .$$

Escolhendo-se uma seqüência $b = (b_1 , \ldots , b_n)$ de inteiros aleatórios (que podem ser negativos), pode-se definir a seqüência $a = (a_1 , \ldots , a_n)$ como segue :

$$a_i = m . b_i + a'_i \quad , \quad i = 1,\ldots,n \qquad \text{(IV-29)}$$

A esta seqüência pode ser aplicada uma iteração para formar a seqüência $p = (p_1 , \ldots , p_n)$, onde :

$$p_i = w . a_i + r_i \quad , \quad i = 1,\ldots,n \qquad \text{(IV-30)}$$

para valores inteiros positivos w e r_i aleatoriamente escolhidos, sendo $w > r_i$.

A seqüência $p = (p_1 , \ldots , p_n)$ é tornada pública, e usada como chave de cifrar mensagens.

A cifração no esquema proposto por Arazi corresponde a adicionar, ao valor numérico da mensagem, a soma dos elementos de um subconjunto da chave pública para formar o criptograma :

$$S = M + \sum_{j \in J} p_j \qquad \text{(IV-31)}$$

onde : S é o criptograma ;

M é o valor numérico decimal do bloco da mensagem, sendo $M \leq (2^h - n + 1).w$;

$p = (p_1, \ldots, p_n)$ é a chave pública de cifrar ;

J é um subconjunto de $\{ 1, 2, \ldots, n \}$.

Juntamente com os elementos da chave de cifrar, deve ser publicado um limite superior para o valor numérico da mensagem.

Vale mencionar que o conhecimento de w e m permite a decifração da mensagem e, por isso, esses parâmetros formam a chave "trapdoor". O receptor autorizado, recebendo S e conhecendo w e m , pode recuperar univocamente a mensagem.

O processo de decifração da mensagem é analisado como segue :

1º CASO :

Dada uma soma qualquer $\sum_{j \in J} a_j$ de elementos da seqüência $(a_i)_{i=1,n}$, e conhecendo o valor m, é possível determinar, univocamente, o conjunto de índices J da seguinte forma :

$$\sum a_j = m . \sum b_j + \sum a'_j \qquad \text{(IV-32)}$$

$$\frac{\sum a_j}{m} = \sum b_j + \frac{\sum a'_j}{m}$$

Como, por construção, $m > \sum_{i=1}^{n} a'_i$, o resto da divisão de Σa_j por m é o próprio valor $\Sigma a'_j$, e assim a conjunto J pode ser recuperado, pois a seqüência $(a'_i)_{i=1,n}$ é supercrescente (recai-se na solução trivial de mochila supercrescente).

2º CASO :

Dado o número $N = K + \Sigma a_j$, onde Σa_j é a soma discutida acima e o valor $K \leq 2^h$, é possível recuperar o valor K e o conjunto de índices J , conhecido m .

Como, por construção, $m > 2^{n+h+2}$, segue-se que :

$$(K + \Sigma a_j) \bmod m = K + \Sigma a'_j \qquad \text{(IV-33)}$$

Uma vez que $K < a'_1$ (pois, por construção $a'_1 \geq 2^h + 1$ e $K \leq 2^h$), o conjunto de índices J pode ser recuperado, após obtido o valor $K + \Sigma a'_j$, usando-se o processo usual, isto é, determinando o maior elemento a'_q possível na seqüência supercrescente tal que :

$$a'_q < K + \Sigma a'_j < a'_{q+1} \qquad \text{(IV-34)}$$

e, então, subtraindo seu valor da soma residual e repetindo-se o processo. Quando for obtido um valor menor que a'_1 , este valor é o próprio K , e desta forma recupera-se o conjunto de índices J , pois q é um elemento deste conjunto.

3º CASO :

Dada uma soma qualquer $\sum_{j \in J} p_j$ de elementos da chave pública $(p_i)_{i=1,n}$, e conhecidos os valores w e m , é possível determinar univocamente o conjunto de índices J , da seguinte forma :

$$\Sigma p_j = w \cdot \Sigma a_j + \Sigma r_j \qquad \text{(IV-35)}$$

$$\frac{\Sigma p_j}{w} = \Sigma a_j + \frac{\Sigma r_j}{w}$$

Como $w > r_i$, então $\sum_{i=1}^{n} r_i < n \cdot w$, logo :

$$\frac{\sum p_j}{w} = K + \sum a_j \qquad \text{(IV-36)}$$

onde : $K = \dfrac{\sum r_j}{w} < n$

Uma vez que, em sistemas práticos, $n << 2^h$, o conjunto J pode ser determinado univocamente para qualquer valor $N = K + \sum a_j$, desde que $K \leq 2^h$, usando o processo descrito no 2º CASO, pois o valor m é conhecido.

4º CASO :

Dada a soma $S = M + \sum_{j \in J} p_j$, sendo M o valor numérico da mensagem, $M \leq (2^h - n + 1).w$, e $(p_i)_{i=1,n}$ o vetor mochila público, tanto M como J podem ser recuperados.

Supondo o valor máximo para M e usando a expressão (IV-35) tem-se :

$$(2^h - n + 1).w + \sum p_j = (2^h - n + 1).w + w \cdot \sum a_j + \sum r_j$$

onde : $\sum r_j \leq (n-1).w + u_j$, para $u_j < w$

(pois $w > r_j$, e então $\sum_{j=1}^{n} r_j < n \cdot w$)

Dividindo-se S por w é obtido o quociente $K + \sum a_j$, onde $K \leq 2^h$, a partir do qual o conjunto de índices J pode ser recuperado. Assim, considerando o valor máximo para M, vem:

$$\frac{M + \sum p_j}{w} = \frac{(2^h - n + 1).w}{w} + \frac{w \cdot \sum a_j}{w} + \frac{\sum r_j}{w}$$

$$= (2^h - n + 1) + (n-1) + \frac{u_j}{w} + \sum a_j$$

$$= 2^h + \frac{u_j}{w} + \sum a_j \quad ; \quad \frac{u_j}{w} < 1$$

Desta forma pode-se escrever :

$$\frac{M + \Sigma p_j}{w} = K + \Sigma a_j \qquad \text{(IV-37)}$$

onde : $K < 2^h + 1$

Por construção $a'_1 \geq 2^h + 1$, e, como $K < a'_1$, então vale o processo descrito no 2º CASO para obtenção do conjunto J .

Uma vez recuperado o conjunto de índices J , pode-se calcular o valor $\Sigma_{j \in J} p_j$, que é subtraído de $S = M + \Sigma p_j$ para então determinar o valor numérico M da mensagem. De posse deste valor, é trivial a obtenção da representação binária da mensagem.

O exemplo a seguir ilustra o criptossistema proposto por ARAZI [12].

IV.2.1.3.2 - EXEMPLO DE APLICAÇÃO

Sejam : $h = 5$ e $n = 4$

Sejam os elementos a'_i , $i=1,...,4$, escolhidos do intervalo :

$$[\ (2^{i}-1).2^{5} + 1\ ;\ 2^{5+i}\ ]$$

$a'_1 = 40$, $a'_2 = 98$, $a'_3 = 230$, $a'_4 = 470$

$a' = (\ 40,\ 98,\ 230,\ 470\ )$

Seja :

$$m \in [\ 2^{n+h+2} + 1\ ,\ 2^{n+h+3} - 1\ ]$$

$$m \in [\ 2049\ ;\ 4095\ ]$$

Escolhido : $m = 2637$.

Sejam também os elementos b_i , $i=1,...,4$, inteiros (positivos ou negativos) aleatoriamente escolhidos :

$b_1 = 3$, $b_2 = 1$, $b_3 = 2$, $b_4 = 1$

$b = (\ 3,\ 1,\ 2,\ 1\ )$

Calculando os elementos a_i , $i=1,...,4$ vem :

$$a_i = m \cdot b_i + a'_i$$

$a_1 = 2637 \times 3 + 40 = 7951$

$a_2 = 2637 \times 2 + 98 = 5372$

$a_3 = 2637 \times 1 + 230 = 2867$

$a_4 = 2637 \times 1 + 470 = 3107$

$a = (\ 7951,\ 5372,\ 2867,\ 3107\ )$

1º - Sem considerar iteração da seqüência $(a_i)_{i=1,4}$

Seja : $w = 1 \quad \therefore \quad r_i = 0 \ , \ i=1,2,3,4$

Como :

$$M \leq (2^{h}-n+1).w = (2^{5}-4+1).1 = 29 \ ,$$

então, para uma mensagem binária de 5 bits igual a 11011 (cujo valor numérico M correspondente é 27), pode ser aplicado o procedimento descrito acima :

- Cifração

O criptograma a ser transmitido é :

$$S = M + \sum_{j \in J} a_j$$

Escolhendo $J = \{ 1, 3, 4 \}$ vem :

$$S = 27 + (7951 + 2867 + 3107) = 13952$$

- Decifração

$S = M + \sum_{j \in J} a_j$, que aplicando mod 2637 vem :

$$13952 \bmod 2637 = (M + \Sigma a_j) \bmod 2637$$

$$767 = M + \Sigma a_j$$

j=4 ,	767 > 470	→	4 ∈ J
j=3 ,	230 < (767-470) < 470	→	3 ∈ J
j=2 ,	(297-230) < 230 (297-230) < 98	→	2 ∉ J
j=1 ,	40 < (297-230) < 98	→	1 ∈ J

Logo : $J = \{ 1, 3, 4 \}$

Desta forma recupera-se a mensagem :

$$M = S - \sum_{j \in J} a_j$$

$$M = 13952 - (a_1 + a_3 + a_4)$$

$$M = 13952 - (7951 + 2867 + 3107)$$

$M = 27$, cuja representação binária é : 11011

2º - Considerando uma iteração para a seqüência $(a_i)_{i=1,4}$

Seja : $w = 6$

Como $r_i < w$, vem :

$$r_1 = 2 \ , \quad r_2 = 1 \ , \quad r_3 = 3 \ , \quad r_4 = 5$$

Então :

$$p_i = w.a_i + r_i$$

$$p_1 = (6 \times 7951) + 2 = 47708$$

$$p_2 = (6 \times 5372) + 1 = 32233$$

$$p_3 = (6 \times 2867) + 3 = 17205$$

$$p_4 = (6 \times 3107) + 5 = 18647$$

$$p = (47708, 32233, 17205, 18647)$$

O valor numérico máximo para a mensagem será:

$$M \leq w.(2^{h-n+1}) = 174$$

Para $M = 160$ vem :

- Cifração

Escolhendo $J = \{ 1, 2, 4 \}$, o criptograma será :

$$S = 160 + (47708 + 32233 + 18647) = 98748$$

- Decifração

$$\frac{S}{w} \mod m = \frac{M + \Sigma p_j}{w} \mod m$$

$$\frac{98748}{6} \mod 2637 = K + \Sigma a'_j \qquad \therefore \quad 636 = K + \Sigma a'_j$$

$j=4$, $636 > 470$ $\rightarrow$ $4 \in J$

$j=3$, $(636-470) < 470$, $(636-470) < 230$ $\rightarrow$ $3 \notin J$

$j=2$, $98 < (636-470) < 230$ $\rightarrow$ $2 \in J$

$j=1$, $40 < (166-98) < 98$ $\rightarrow$ $1 \in J$

Logo : $J = \{ 1, 2, 4 \}$

Assim a mensagem pode ser recuperada :

$$M = 98748 - (p_1 + p_2 + p_4) \qquad \therefore \quad M = 160$$

IV.2.1.3.3 - COMENTÁRIOS

O sistema criptográfico proposto por ARAZI [12] apresenta uma formulação um pouco diferente do SCMH, tanto no que se refere à geração da chave pública, quanto aos processos de cifração e decifração das mensagens.

No criptossistema de Arazi a cifração de uma mensagem é feita adicionando-se ao valor numérico decimal da mensagem uma soma de elementos aleatórios da chave pública, caracterizando esse sistema como "Mochila Aditiva". Esse esquema de cifração possibilita cifrar a mesma mensagem de 2^n modos diferentes usando a mesma mochila de n elementos, permitindo representação múltipla da mensagem e gerando homofonia para dificultar a criptoanálise.

Além de permitir representação múltipla da mensagem, outra vantagem significativa desse esquema de "soma aleatória" é que a maior parte do processo de cifração independe do texto claro. Os elementos da mochila que serão adicionados ao texto claro podem, em princípio, ser selecionados do arquivo conhecido publicamente, somados e armazenados. O texto claro pode aparecer somente no último estágio do processo e ser somado ao valor armazenado, formando então o criptograma, o que, sem dúvida, pode aumentar drasticamente a velocidade de cifração. O esquema é muito eficiente no sentido de que o criptograma gerado não é muito maior (em bits) que o texto claro correspondente, isto é, a expansão de dados é moderada, enquanto é mantido um razoável critério de segurança. (A segurança deste sistema depende fortemente da escolha dos parâmetros w e r_i para formar a chave pública de cifrar.)

Quanto à decifração, o sistema de Arazi apresenta um processo fácil de volta única, baseado nos parâmetros secretos.

O esquema proposto por Arazi muito provavelmente resistirá aos ataques de recuperação da informação "trapdoor" [25], [27] e [29], uma vez que a chave pública é obtida por um processo diferente do empregado no SCMH. Nada se pode garantir, no entanto, em relação aos ataques por reduções sucessivas [6], [21] e [26] e nem aos ataques a mochilas de baixa densidade [35] e [43].

IV.2.2 - CHAVE SECRETA NÃO-SUPERCRESCENTE

Em 1982 WILLETT [30] publicou um dos primeiros trabalhos propondo a utilização de seqüências não supercrescentes no desenvolvimento de sistemas criptográficos de chave pública tipo mochila. No ano anterior, porém, PAZ DE LIMA [47] já havia apresentado, sem no entanto publicar, uma formulação para criptossistemas de chave pública sem fazer uso de seqüências supercrescentes. A partir de então, surgiram novas generalizações para o SCMH, nas quais a idéia básica é a construção do sistema sem usar seqüências supercrescentes com a finalidade principal de evitar o ataque criptoanalítico de SHAMIR [27] e similares.

IV.2.2.1 - MOCHILA "ÚTIL"

O conceito de mochila "inútil" foi introduzido em 1982 quando DESMEDT, VANDEWALLE e GOVAERTS [38] classificaram as mochilas em função de sua utilidade criptográfica. Os recentes desenvolvimentos sobre o problema mochila permitiram uma definição mais geral, fazendo uma distinção entre as mochilas "inúteis" do ponto de vista teórico e do ponto de vista prático. Segundo aqueles autores, as mochilas que geram sistemas não injetivos são "inúteis" tanto do ponto de vista teórico como do ponto de vista prático. O conjunto de mochilas "úteis" do ponto de vista teórico pode ser dividido em dois subconjuntos : as mochilas "úteis" e "inúteis" do ponto de vista prático. Mochila "útil" do ponto de vista prático significa que chaves de cifrar podem ser geradas em tempo polinomial (com o grau do polinômio não muito elevado).

Em 1983/1984 DESMEDT, VANDEWALLE e GOVAERTS [17] e [37] propuseram uma generalização para o sistema criptográfico de chave pública tipo mochila, utilizando, em seu algoritmo, resultados da álgebra linear e mapeamentos estendidos como informação "trapdoor" para o problema mochila. Um dos objetivos desse novo sistema é reduzir o subconjunto de mochilas "inúteis", em favor das mochilas "úteis", como mostrado a seguir.

IV.2.2.1.1 - CONCEITUAÇÃO BÁSICA

O sistema criptográfico tipo mochila proposto por DESMEDT, VANDEWALLE e GOVAERTS [17] e [37], utiliza equações lineares e mapeamento estendido (Vide Definição IV-1) para gerar a chave pública de decifrar a partir de uma mochila "útil" não supercrescente.

Neste sistema a operação de cifrar consiste no cálculo do produto interno de dois vetores :

$$S^{(n)} = a^{(n)} \cdot x^T \qquad \text{(IV-38)}$$

onde : $x = (x_1,\ldots,x_n)$ é o vetor binário que representa o texto claro ;

$a^{(n)} = (a_1^{(n)},\ldots,a_n^{(n)})$ é a chave pública ;

$S^{(n)}$ é o criptograma transmitido.

A decifração consiste, primeiramente, na construção de n equações lineares independentes, usando parâmetros secretos . Em seguida, resolve-se este sistema de equações empregando, por exemplo, o método clássico de eliminação de Gauss, para determinar o vetor $x = (x_1,\ldots,x_n)$. O conjunto das equações lineares é definido pelo sistema (IV-39), e a matriz n x n é chamada de matriz D de decifração.

$$\begin{bmatrix} R^{(1)} \\ R^{(2)} \\ \vdots \\ R^{(n-1)} \\ S^{(n)} \end{bmatrix} = \begin{bmatrix} b_1^{(1)} & \cdots & b_n^{(1)} \\ b_1^{(2)} & \cdots & b_n^{(2)} \\ \vdots & & \\ b_1^{(n-1)} & \cdots & b_n^{(n-1)} \\ a_1^{(n)} & \cdots & a_n^{(n)} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \\ x_n \end{bmatrix} \qquad \text{(IV-39)}$$

As n-1 equações extras em (IV-39), necessárias para a decifração das mensagens, são obtidas a partir de $S^{(n)}$ e $a^{(n)}$, calculando-se, sequencialmente, $b^{(n-1)}$ e $R^{(n-1)}$; $S^{(n-1)}$, $a^{(n-1)}$, $b^{(n-2)}$ e $R^{(n-2)}$; $S^{(n-2)}$, $a^{(n-2)}$, $b^{(n-3)}$ e $R^{(n-3)}$; ...; $S^{(2)}$, $a^{(2)}$, $b^{(1)}$ e $R^{(1)}$.

Vale mencionar que no processo de obtenção da chave pública de cifrar $a^{(n)} = (a_1^{(n)},\ldots,a_n^{(n)})$ os vetores são gerados exatamente em sentido oposto ao usado no processo de decifração de uma mensagem (descrito adiante). Assim, são gerados, sequencialmente, os vetores $b^{(1)}$, $a^{(2)}$, $b^{(2)}$, $a^{(3)}$,..., $b^{(n-1)}$, $a^{(n)}$ (este último é a chave pûblica).

No processo de decifração será usado um mapeamento estendido a fim de gerar uma nova equação linear em x para o sistema (IV-39), usando parâmetros secretos conhecidos apenas pelo receptor autorizado.

Definição IV-1 : Mapeamento estendido

Um mapeamento f_{j-1} é um mapeamento estendido de um subconjunto de $\mathbb{Z}$ em $\mathbb{Z}$ se, e somente se, para cada vetor binário $x = (x_1,\ldots,x_n)$, $x_i=0$ ou 1 para i=1,...,n, e considerados os vetores $a^{(n)}$, $b^{(n-1)}$,..., $b^{(j)}$ de n elementos inteiros,

$$f_{j-1}(\Sigma x_i.a_i^{(j)}) = \Sigma (x_i \cdot f_{j-1}(a_i^{(j)}))$$

ou (IV-40)

$$f_{j-1} (\Sigma x_i.a_i^{(n)}, \Sigma x_i.b_i^{(n-1)},\ldots, \Sigma x_i.b_i^{(j)}) =$$

$$= \Sigma x_i \cdot (f_{j-1} (a_i^{(n)}, b_i^{(n-1)},\ldots, b_i^{(j)}))$$

Definição IV-2 : Mapeamento estendido simplificado

Um mapeamento f_{j-1} é um mapeamento estendido simplificado se, e somente se :

1º - $S^{(j)}$ e $a^{(j)}$ forem obtidos por combinação linear com inteiros e^j_k ($j \leq k \leq n$) da seguinte forma :

$$S^{(j)} = e^j_n S^{(n)} + e^j_{n-1} R^{(n-1)} + \ldots + e^j_j R^{(j)} \qquad \text{(IV-41)}$$

$$a^{(j)} = e^j_n a^{(n)} + e^j_{n-1} b^{(n-1)} + \ldots + e^j_j b^{(j)}$$

$$j = n-1, \ldots, 2$$

2º - Um mapeamento estendido f_{j-1} é usado tal que, para cada vetor binário $\mathbf{x}$, tem-se :

$$f_{j-1}\left(\Sigma\, x_i . a_i^{(j)} \right) = \Sigma\, x_i \,.\, \left(f_{j-1} \left(a_i^{(j)} \right) \right) \qquad \text{(IV-42)}$$

Para um mapeamento estendido simplificado assim definido, tem-se :

$$R^{(j-1)} = b^{(j-1)} . x^T \qquad \text{(IV-43)}$$

porque $S^{(j)} = a^{(j)} . x^T$ pela equação (IV-41).

A expressão (IV-40) descreve como o mapeamento f_{j-1} sobre os inteiros $a_i^{(j)}$ deve ser estendido aos inteiros $S^{(j)} = a^{(j)} . x^T$, tal que uma nova equação para o sistema (IV-39) seja gerada.

Considerando um mapeamento estendido f_{j-1}, conhecido apenas pelo receptor autorizado, tem-se que :

$$R^{(j-1)} = f_{j-1}\left(S^{(n)}, R^{(n-1)}, \ldots, R^{(j)} \right) \qquad \text{(IV-44)}$$

$$b_i^{(j-1)} = f_{j-1}\left(a_i^{(n)}, b_i^{(n-1)}, \ldots, b_i^{(j)} \right) \qquad 1 \leq i \leq n$$

Pela expressão (IV-40) vem :

$$R^{(j-1)} = b^{(j-1)} \cdot x^T \qquad \text{(IV-45)}$$

e assim pode ser obtida a próxima equação linear para o sistema (IV-39).

É evidente que o mapeamento estendido f_{j-1} deve ser não linear, e também fácil de ser calculado pelo receptor autorizado. Vale mencionar que o conjunto de mapeamentos estendidos para aplicações práticas é reduzido, devido às propriedades que deve possuir. Como ilustração do uso de mapeamentos estendidos pode ser citada a transformação modular M-dominante (Vide Definição III-7).

Repetindo-se, sucessivamente, o processo para obtenção das n-1 equações extras, compõe-se o sistema de n equações lineares, que, resolvido, fornecerá o vetor $x = (x_1, \ldots, x_n)$ representativo da mensagem.

É importante observar que a matriz D de decifração definida no sistema (IV-39) é independente do criptograma e, por isso, pode ser calculada uma única vez e armazenada, proporcionando alta velocidade no processo de decifração.

O esquema de Merkle-Hellman é um caso especial do sistema criptográfico apresentado em [17] e [37], pois utiliza seqüência supercrescente para gerar a chave pública e considera transformações modulares M-dominantes

O processo de decifração de uma mensagem, no sistema criptográfico apresentado em [17] e [37], pode ser descrito como:

- Partindo do vetor chave pública $a^{(n)}$, gerar um segundo vetor $b^{(n-1)}$ usando um mapeamento estendido :

$$b_i^{(n-1)} = f_{n-1} (a_i^{(n)}) \quad , \quad i = 1,\ldots,n$$

- Usar este mapeamento estendido para determinar $R^{(n-1)}$ a partir de $S^{(n)}$:

$$R^{(n-1)} = f_{n-1} (S^{(n)})$$

- Escolher um vetor qualquer $a^{(n-1)}$ no plano $(a^{(n)}, b^{(n-1)})$ usando combinação linear com inteiros e_k^j $(j \leq k \leq n)$:

$$a^{(n-1)} = e_n^{n-1} a^{(n)} + e_{n-1}^{n-1} b^{(n-1)}$$

- Aplicar a mesma combinação linear à $(S^{(n)}, R^{(n-1)})$ para obter $S^{(n-1)}$:

$$S^{(n-1)} = e_n^{n-1} S^{(n)} + e_{n-1}^{n-1} R^{(n-1)}$$

- De posse do valor $S^{(n-1)}$ e do vetor $a^{(n-1)}$, aplicar um mapeamento estendido f_{n-2} para determinar :

$$b_i^{(n-2)} = f_{n-2} (a_i^{(n-1)}) \quad , \quad i = 1,\ldots,n$$

$$R^{(n-2)} = f_{n-2} (S^{(n-1)})$$

- Escolher um vetor $a^{(n-2)}$ no subespaço gerado pelos vetores $a^{(n)}$, $b^{(n-1)}$ e $b^{(n-2)}$, usando combinação linear para determinar :

$$S^{(n-2)} = e_n^{n-2} S^{(n)} + e_{n-1}^{n-2} R^{(n-1)} + e_{n-2}^{n-2} R^{(n-2)}$$

$\vdots$

- Para obter $R^{(j-1)}$ e $b^{(j-1)}$, $1 < j < n$, calculam-se primeiramente :

$$a^{(j)} = e_n^j \, a^{(n)} + e_{n-1}^j \, b^{(n-1)} + \ldots + e_j^j \, b^{(j)}$$

$$S^{(j)} = e_n^j \, S^{(n)} + e_{n-1}^j \, R^{(n-1)} + \ldots + e_j^j \, R^{(j)}$$

e finalmente :

$$b_i^{(j-1)} = f_{j-1} \left(a_i^{(j)} \right) \quad , \quad i = 1, \ldots, n$$

$$R^{(j-1)} = f_{j-1} \left(S^{(j)} \right)$$

Deste modo são obtidas as $n-1$ equações extras necessárias para formar o sistema (IV-39).

O processo descrito acima implica, explícita ou implicitamente, as seguintes exigências :

1º - Os vetores $a^{(j)}$ e $b^{(j)}$ devem ter coeficientes inteiros ;

2º - O vetor $a^{(j)}$ deve pertencer ao subespaço gerado pelos vetores $\left(a^{(n)}, b^{(n-1)}, \ldots, b^{(j)} \right)$;

3º - Os vetores $a^{(n)}, b^{(n-1)}, \ldots, b^{(1)}$ devem formar um conjunto linearmente independente.

Como mencionado anteriormente, um dos objetivos do sistema criptográfico apresentado em [17] e [37] é aumentar o subconjunto de mochilas criptográficas "úteis". Por isso, o algoritmo de construção de chaves públicas deve permitir gerar tantas chaves de cifrar quantas forem possíveis (é claro que estas chaves precisam satisfazer os requisitos necessários ao processo de decifração).

Durante o processo de obtenção da chave pública são gerados 2n-2 vetores, que não formam uma base no espaço inteiro n-dimensional. O algoritmo controla a dependência linear neste conjunto de 2n-2 vetores e a cada momento o maior conjunto de vetores linearmente independentes é atualizado e armazenado. Mais precisamente, durante a iteração, são eliminados os vetores linearmente dependentes no conjunto formado pelos vetores $(b^{(j-1)}, \ldots, b^{(1)}, a^{(j)}, \ldots, a^{(1)})$, começando-se a eliminação pelos vetores $a^{(i)}$, $i=1,\ldots,j$.

Concluído o processo de geração da chave pública, a escolha final deve ser um conjunto de n vetores linearmente independentes, $a^{(n)}, b^{(n-1)}, b^{(n-2)}, \ldots, b^{(1)}$, pois de outra forma estaria conflitante com as condições exigidas pelo processo de decifração, uma vez que o sistema (IV-39) só admite solução se suas equações forem linearmente independentes. Vale dizer que os graus de liberdade do algoritmo são criados pelos vetores linearmente dependentes.

IV.2.2.1.2 - COMENTÁRIOS

O sistema criptográfico de chave pública proposto por DESMEDT, VANDEWALLE e GOVAERTS [17] e [37], é uma generalização do criptossistema mochila de MERKLE-HELLMAN [3], e utiliza equações lineares e mapeamentos estendidos para fornecer uma informação "trapdoor" para o problema da mochila. Neste sistema a chave pública de cifrar é gerada a partir de uma mochila "útil" não supercrescente. O processo de decifração de uma mensagem, após ser obtida a matriz de decifração com a geração de n-1 equações lineares extras usando parâmetros secretos, recai no cálculo matricial, que requer tempo polinomial em função do número de equações e do tamanho dos inteiros que compõem a matriz. Como a matriz de decifração independe do criptograma, ela pode ser gerada uma única vez e armazenada, propiciando, assim, uma decifração rápida.

Muitos algoritmos de chave pública tipo mochila são casos especiais do sistema criptográfico geral apresentado em [17] e [37]. Deve-se ressaltar que este esquema só terá sentido se puder ser garantida uma segurança maior que dos esquemas mochila já quebrados.

Pode-se discutir a segurança do criptossistema apresentado em [17] e [37] no contexto dos principais ataques existentes contra os esquemas tipo mochila.

O ataque de recuperação da informação "trapdoor", proposto por SHAMIR [27] e outros [25] e [29], contra o esquema básico de Merkle-Hellman, não se aplica ao esquema apresentado em [17] e [37], porque aquele ataque utiliza, explicitamente, a propriedade da seqüência inicial ser supercrescente a fim de poder empregar o algoritmo de LENSTRA [48]. Uma observação similar é verdadeira também sobre o ataque de ADLEMAN [34], que se baseia na estrutura da chave de decifrar, supercrescente ou Graham-Shamir.

Quanto aos ataques por reduções sucessivas [6], [21] e [26], não se pode garantir que o sistema seja resistente a eles.

Outro ataque que pode ter sucesso contra o esquema geral apresentado em [17] e [37] é o ataque a mochilas de baixa densidade [35] e [43].

Deve-se ter sempre em mente que a discussão acima só é verdadeira se os parâmetros escolhidos forem suficientemente aleatórios. Em outras palavras, escolhendo-se parâmetros muito especiais no processo de construção da chave pública pode-se obter, por exemplo, chaves de cifrar supercrescentes ou as mesmas chaves de cifrar como no SCMH ou outros esquemas fracos.

Quanto aos aspectos práticos do esquema proposto em [17] e [37], pode-se afirmar que a velocidade de cifração permanece a mesma, como em outros sistemas mochila [2], [3] e [12]. O processo de decifração pode ser acelerado empregando-se as técnicas discutidas anteriormente, pois a operação de decifração pode ser muito lenta em alguns casos. A questão principal sobre a velocidade é a existência de um compromisso aceitável entre decifração rápida e segurança.

IV.2.2.2 - MOCHILA ARBITRÁRIA QUALQUER

Muitos criptossistemas de chave pública, baseados no algoritmo da mochila, executam, basicamente, o seguinte procedimento :

1º - Escolher uma seqüência "fácil" injetiva ;

2º - Utilizar multiplicações modulares iterativas para disfarçar (esconder) a propriedade de supercrescimento dessa seqüência ; e

3º - Publicar a mochila aparentemente aleatória resultante como chave de cifrar.

Em 1983 SHAMIR [32] propôs um algoritmo criptográfico que permitiu modificar o primeiro passo desse procedimento, passando a ser :

1º - Escolher uma seqüência arbitrária qualquer ;

isto é, a mochila inicial não precisa ser injetiva, e seus elementos podem ser de valores arbitrários. (Apesar de não ter sido mencionada explicitamente em [32], para o sistema funcionar é preciso que os elementos da mochila inicial sejam não nulos e diferentes entre si). Esta mochila é transformada em um sistema criptográfico com passagem secreta ("trapdoor") e pode ser empregada na criptografia de chave pública.

O método de Shamir utiliza seqüência não supercrescente e pode ser usada com qualquer processo iterativo de embaralhamento, uma vez que todos os problemas mochila intermediários apresentam a mesma solução, e seus elementos são, aparentemente, aleatórios.

IV.2.2.2.1 - CONCEITUAÇÃO BÁSICA

Seja $(a_1^{(1)}, \ldots, a_n^{(1)})$ um vetor mochila inicial arbitrário com as seguintes restrições : $a_i^{(1)} \neq 0$, $i = 1, \ldots, n$ e $a_i^{(1)} \neq a_j^{(1)}$, $i \neq j$, $i,j = 1, \ldots, n$.

Seja $(a_1^{(j)}, \ldots, a_n^{(j)})$ o vetor obtido após j-1 multiplicações modulares.

Sejam, ainda, $M^{(j)}$ e $w^{(j)}$ o j-ésimo módulo e multiplicador, respectivamente. Define-se, então :

$$a_i^{(j+1)} = w^{(j)} . a_i^{(j)} \bmod M^{(j)} \quad , \quad i = 1, \ldots, n \qquad \text{(IV-46)}$$

onde os valores inteiros $M^{(j)}$ e $w^{(j)}$ são arbitrários, porém satisfazendo :

$$M^{(j)} > \sum_{i=1}^{n} a_i^{(j)} \qquad \text{(IV-47)}$$

$$1 < w^{(j)} < M^{(j)}$$
$$(w^{(j)}, M^{(j)}) = 1 \qquad \text{(IV-48)}$$

A multiplicação modular expressa em (IV-46) é repetida n-1 vezes, e o vetor resultante $(a_1^{(n)}, \ldots, a_n^{(n)})$ é publicado como sendo a chave de cifrar.

Para cifrar uma mensagem com texto claro representado pelo vetor binário $x = (x_1, \ldots, x_n)$, $x_i = 0$ ou 1, o emissor calcula a soma :

$$\sum_{i=1}^{n} x_i . a_i^{(n)} = S^{(n)} \quad , \qquad \text{(IV-49)}$$

e envia o criptograma $S^{(n)}$ para o receptor autorizado.

Para decifar $S^{(n)}$ o receptor multiplica a equação (IV-49) pelo inverso de $w^{(n-1)}$ mod $M^{(n-1)}$ (o inverso existe pois $w^{(n-1)}$ e $M^{(n-1)}$ são primos entre si). Cada $a_i^{(n)}$ é transformado de volta em $a_i^{(n-1)}$, e $S^{(n)}$ é alterado para um novo valor $S^{(n-1)}$:

$$a_i^{(n-1)} = a_i^{(n)} . (w^{(n-1)})^{-1} \bmod M^{(n-1)} , \quad i=1,\ldots,n \qquad \text{(IV-50)}$$

$$S^{(n-1)} = S^{(n)} . (w^{(n-1)})^{-1} \bmod M^{(n-1)} \qquad \text{(IV-51)}$$

$$\sum_{i=1}^{n} x_i . a_i^{(n-1)} = S^{(n-1)} \bmod M^{(n-1)} \qquad \text{(IV-52)}$$

Já que cada x_i é no máximo igual a 1(um), e $M^{(n-1)}$ é maior que a soma de todos os elementos $a_i^{(n-1)}$, então a equação (IV-52) pode ser escrita como :

$$\sum_{i=1}^{n} x_i . a_i^{(n-1)} = S^{(n-1)} \qquad \text{(IV-53)}$$

Repetindo este processo n-1 vezes, o receptor pode reunir n equações não-modulares inteiras com n incógnitas para formar o sistema :

$$\sum_{i=1}^{n} x_i . a_i^{(j)} = S^{(j)} , \quad j=1,\ldots,n \qquad \text{(IV-54)}$$

Como este sistema tem grande probabilidade de ser não-singular, pois os parâmetros M e w de cada iteração podem ser escolhidos de modo que as equações sejam linearmente independentes, então o receptor pode resolver o sistema, usando a matriz inversa dos coeficientes, e determinar $x = (x_1,\ldots,x_n)$, que é a solução procurada.

Em vez de resolver as equações sobre os racionais, o receptor pode reduzir as equações (mod 2) e resolvê-las sobre GF(2). As equações reduzidas somente contêm os bits menos significativos de $a_i^{(j)}$, i=1,...,n , e de $S^{(j)}$, e eles são muito mais fáceis de armazenar e manipular.

Entretanto, para matrizes binárias aleatórias a probabilidade de não-singularidade é de, aproximadamente, 0.3 (30%) conforme mostrado em [32], e por isso é necessário gerar algumas chaves aleatórias antes de se obter uma chave útil.

O inverso (A^{-1}) da matriz A de bits menos significativos dos elementos $a_i^{(j)}$ pode ser pré-computado durante a fase de geração da chave pública e, assim, o procedimento de decifração consistirá em coletar os bits menos significativos dos números $S^{(j)}$ para formar um vetor, e multiplicar este vetor pela matriz A^{-1} binária fixa de dimensão (n x n), como mostrado no exemplo a seguir.

Para um criptossistema mochila ser seguro deve ter, no mínimo, 100 bits x_i desconhecidos e, assim, a matriz de decifração conterá, no mínimo, 10.000 bits (n x n = 100 x 100). Existe, porém, uma maneira fácil de controlar a estrutura dessa matriz e transformá-la em uma matriz particular escolhida.

Sejam $M^{(1)},\ldots, M^{(n-1)}$ números ímpares. Após multiplicar $a_1^{(j)},\ldots, a_n^{(j)}$ por $w^{(j)}$ e reduzí-los mod $M^{(j)}$, pode-se somar $M^{(j)}$ seletivamente a qualquer subconjunto de elementos do vetor resultante, já que essas ocorrências extras de $M^{(j)}$ serão eliminadas, durante a fase de decifração, pela multiplicação inversa mod $M^{(j)}$.

Como $M^{(j)}$ é ímpar, o bit menos significativo de $a_i^{(j+1)}$ é removido quando $M^{(j)}$ é adicionado a ele, e, assim, podem-se selecionar independentemente todos os elementos da matriz. Em particular, pode-se escolher um sistema mochila para o qual a matriz de coeficientes é a própria matriz identidade ; o texto claro, neste caso, será simplesmente a seqüência dos bits menos significativos dos valores intermediários $S^{(j)}$.

Entretanto, esta técnica introduz uma pequena parcela do conhecimento da estrutura nos sistemas mochila intermediários, e, assim, para conseguir a maior segurança possível, parece ser aconselhável deixar a matriz aleatória.

No exemplo a seguir é mostrado como obter uma matriz identidade usando a técnica descrita acima.

No método criptográfico proposto por SHAMIR [32], o transmissor calcula o criptograma usando a última mochila do processo de geração da chave pública (chave de cifrar), e envia o resultado ao receptor autorizado. Este, então, executa as transformações modulares inversas para obter o sistema de n equações inteiras não-modulares, e determinar $x = (x_1, \ldots, x_n)$ que é a solução procurada.

IV.2.2.2.2 - EXEMPLOS DE APLICAÇÃO

1º - Matriz Arbitrária

Seja : $a^{(1)} = (3, 8, 11)$ o vetor inicial não injetivo do sistema mochila.

Sejam os parâmetros :

$$M^{(1)} = 25 \quad (> 3+8+11 = 22)$$

$$w^{(1)} = 14 \qquad \therefore \qquad (w^{(1)})^{-1} = 9 \bmod 25$$

Operando este sistema com multiplicações modulares obtém-se :

$$a_i^{(2)} = a_i^{(1)} \cdot w^{(1)} \bmod \mathbf{M}^{(1)} \quad , \; i = 1,2,3$$

$$a^{(2)} = (17, 12, 4)$$

Escolhendo : $M^{(2)} = 37 \quad (> 17+12+4 = 33)$

$$w^{(2)} = 17 \qquad \therefore \quad (w^{(2)})^{-1} = 24 \bmod 37$$

vem :

$$a_i^{(3)} = a_i^{(2)} \cdot w^{(2)} \bmod \mathbf{M}^{(2)} \quad , \; i = 1,2,3$$

$$a^{(3)} = (30, 19, 31)$$

Então, para qualquer criptograma $S^{(3)}$, o sistema de equações é :

$$\begin{cases} 3 x_1 + 8 x_2 + 11 x_3 = S^{(1)} \\ 17 x_1 + 12 x_2 + 4 x_3 = S^{(2)} \\ 30 x_1 + 19 x_2 + 31 x_3 = S^{(3)} \end{cases}$$

Este sistema pode ser resolvido sobre os racionais, porém é mais simples reduzí-lo mod 2 , obtendo-se :

$$\begin{cases} 1\,x_1 + 0\,x_2 + 1\,x_3 = \tilde{s}^{(1)} \\ 1\,x_1 + 0\,x_2 + 0\,x_3 = \tilde{s}^{(2)} \\ 0\,x_1 + 1\,x_2 + 1\,x_3 = \tilde{s}^{(3)} \end{cases} ,$$

onde $\tilde{s}^{(j)}$ é o bit menos significativo de $s^{(j)}$.

Assim, pode-se determinar x para qualquer vetor $\tilde{s}^{(j)}$:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}^{-1} \cdot \begin{bmatrix} \tilde{s}^{(1)} \\ \tilde{s}^{(2)} \\ \tilde{s}^{(3)} \end{bmatrix}$$

Note-se que este sistema de equações é não-singular , apesar do vetor mochila inicial (3, 8, 11) ser não injetivo. Se, no entanto, o sistema fosse singular, o processamento poderia ser repetido até que se obtivesse um sistema linearmente independente.

Considerando o vetor mensagem x = (1, 1, 0), e utilizando a equação (IV-49), o criptograma será :

$$s^{(3)} = 1x30 + 1x19 + 0x31 = 49 ,$$

e operando módulo 2 tem-se : $\tilde{s}^{(3)} = 1$

Utilizando as multiplicações modulares inversas vem :

$$s^{(j)} = s^{(j+1)} \cdot (w^{(j)})^{-1} \mod M^{(j)} \qquad j = 2,1$$

$$s^{(2)} = 49 \times 24 \mod 37 = 29 \quad \therefore \quad \tilde{s}^{(2)} = 1$$

$$s^{(1)} = 29 \times 9 \mod 25 = 11 \quad \therefore \quad \tilde{s}^{(1)} = 1$$

Assim, vem :

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ 2 \end{bmatrix}$$

Aplicando mod 2 obtém-se : $(x_1, x_2, x_3) = (1, 1, 0)$

Desta forma a mensagem foi recuperada facilmente.

2º - Matriz Identidade

Seja o vetor inicial : $a^{(1)} = (3, 8, 12)$

Sejam escolhidos : $M^{(1)} = 25 \ (> 3+8+12=23)$, ímpar

$w^{(1)} = 14 \ \therefore \ (w^{(1)})^{-1} = 9 \bmod 25$

Obtém-se na primeira iteração :

$$a^{(2)} = (17, 12, 18) \ ,$$

que somando-se 25 aos dois primeiros elementos vem :

$$a^{(2)'} = (42, 37, 18) \ .$$

Agora pode-se escolher :

$M^{(2)} = 101 \ (> 42+37+18=97)$

$w^{(2)} = 23 \ \therefore \ (w^{(2)})^{-1} = 22 \bmod 101$

Obtém-se na segunda iteração :

$$a^{(3)} = (57, 43, 10) \ ,$$

que somando-se 101 a todos os elementos vem :

$$a^{(3)'} = (158, 144, 111)$$

Desta forma, as três seqüências possuem a estrutura desejada de bits menos significativos, (matriz identidade), e assim a solução do sistema de equações torna-se trivial :

$$\begin{matrix} (\ 3, & 8, & 12 \ ) \\ (\ 42, & 37, & 18 \ ) \\ (158, & 144, & 111 \ ) \end{matrix} \Rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Para a mensagem $x = (1, 0, 1)$, o criptograma correspondente será :

$$s^{(3)} = 158 + 111 = 269$$

Operando as multiplicações modulares inversas tem-se :

$$S^{(j)} = S^{(j+1)} \cdot (w^{(j)})^{-1} \bmod M^{(j)} \quad , \quad j = 2,1$$

$$S^{(2)} = 269 \times 22 \bmod 101 = 60$$

$$S^{(1)} = 60 \times 9 \bmod 25 = 15$$

Aplicando módulo 2 vem :

$$S^{(3)} = 269 \rightarrow \tilde{S}^{(3)} = 1$$

$$S^{(2)} = 60 \rightarrow \tilde{S}^{(2)} = 0$$

$$S^{(1)} = 15 \rightarrow \tilde{S}^{(1)} = 1$$

Assim, vem :

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

$$(x_1, x_2, x_3) = (1, 0, 1)$$

Desta forma a mensagem foi recuperada facilmente.

IV.2.2.2.3 - COMENTÁRIOS

O sistema criptográfico de chave pública tipo mochila proposto por SHAMIR [32] é uma generalização para o SCMH.

No sistema de Shamir, a mochila inicial não é supercrescente, nem precisa ser injetiva, podendo ser usada uma mochila qualquer com elementos distintos de valores arbitrários. (Para garantir que o método funcione é preciso começar com um vetor de elementos não nulos diferentes entre si.)

No processo de obtenção da chave pública de cifrar as equações geradas são modulares, mas na decifração, ao contrário, todas as equações são inteiras não-modulares e, por isso, é válido usar a matriz inversa para determinar a solução do problema mochila, isto é, recuperar a mensagem.

O usuário deste sistema pode controlar a escolha dos parâmetros w e M usados em cada iteração, de modo que a matriz dos coeficientes tenha inversa (as n seqüências geradas precisam ser linearmente independentes). Deve, ainda, evitar que a seqüência final (chave pública) seja uma mochila supercrescente ou tenha elemento dominante; a chave de cifrar deve ser difícil, porém injetiva.

A grande vantagem do esquema proposto por Shamir é a utilização de mochilas arbitrárias para começar o processo de geração da chave pública, permitindo, desta forma, utilizar, para fins criptográficos, aqueles vetores que antes eram considerados "inúteis".

Os criptossistemas mochila que utilizam seqüências supercrescentes com multiplicações modulares, [3], [10], [12], ... podem ser considerados casos especiais do Sistema Criptográfico de Mochila Arbitrária de SHAMIR [32]. Assim, qualquer ataque criptoanalítico bem sucedido sobre este último também quebrará os outros, mas não necessariamente vice-versa.

Para desenvolver o seu criptossistema, Shamir observou que a técnica de multiplicação modular pode propiciar uma informação "trapdoor" para sistemas mochila e, por isso, não é necessário usar mochilas iniciais "fáceis-de-resolver". Um resultado desta observação é que o criptossistema Merkle-Hellman pode ser enfraquecido, em vez de fortalecido, quando são utilizadas muitas multiplicações modulares, já que elas introduzem novos "trapdoors" não intencionais no sistema mochila.

O criptossistema Mochila Aleatória de Shamir é, certamente, mais seguro que o sistema criptográfico de Merkle e Hellman de múltipla iteração, uma vez que não se supõe que o vetor mochila inicial seja supercrescente, e, desta forma, os ataques de recuperação da informação "trapdoor" [25], [27], [29] e [34], que se baseiam no fato da mochila inicial ser supercrescente para poder utilizar o algoritmo de LENSTRA [48], não serão aplicáveis.

Nada pode ser garantido quanto à resistência do método aos ataques por reduções sucessivas [6], [21] e [26], e nem aos ataques a mochilas de baixa densidade [35] e [43].

IV.2.2.3 - SISTEMA UTILIZANDO TRANSFORMAÇÃO MODULAR NÃO M-DOMINANTE E INCORPORAÇÃO DE RUÍDO

O SCMH e outros criptossistemas mochila [10], [32] , [37], ... utilizam transformações modulares M-dominantes no processo de geração da chave pública de cifrar. Este tipo de transformação pode tornar tais criptossistemas inseguros , pois os ataques criptoanalíticos de recuperação da informação "trapdoor",[25], [27], [29] e [34], utilizam este fato para quebrar o sistema.

Em 1983 BRICKELL [19] propôs um sistema criptográfico, baseado no algoritmo da mochila, que parece ser seguro aos ataques criptoanalíticos que exploram a propriedade de M-dominância. O sistema proposto utiliza a mesma idéia básica do criptossistema de Merkle-Hellman, mas introduz duas modificações :

1ª - O módulo M não é maior que a soma dos elementos da mochila inicial fácil ;

2ª - É utilizado um vetor de ruídos para incorporar aleatoriedade ao sistema.

A seguir é apresentada a formulação do sistema proposto por Brickell.

IV.2.2.3.1 - CONCEITUAÇÃO BÁSICA

No sistema criptográfico proposto por BRICKELL [19] , sejam consideradas as seguintes variáveis para o processo de geração da chave pública de cifrar :

n = tamanho do vetor mensagem ,
k = tamanho do vetor de ruídos ,
r , q = inteiros positivos .

Seja ainda a variável inteira t satisfazendo :

$$t = \lceil \log_2 (n+k) \rceil + 1 \qquad \text{(IV-55)}$$

onde o símbolo $\lceil \theta \rceil$ indica o menor inteiro I , tal que $I \geq \theta$.

Escolher (n+k) elementos $a'_1,\ldots a'_n, b'_1,\ldots,b'_k$, um módulo M e um multiplicador w satisfazendo :

$$a'_i = r_i\, 2^{n+2t+q} + 2^{i-1+2t+q} + q_i \quad , \; 1 \leq i \leq n \qquad \text{(IV-56)}$$

$$b'_i = s_j\, 2^{n+2t+q} + p_j \qquad 1 \leq j \leq k \qquad \text{(IV-57)}$$

$$M = u\, 2^{2t+q} + 2^{t+q} + v \qquad \text{(IV-58)}$$

$$\text{m.d.c.} \; (w, M) = 1 \quad , \quad w > 0 \quad , \quad w \in \mathbb{Z} \qquad \text{(IV-59)}$$

onde r_i , q_i , s_j , p_j , u , v são inteiros positivos escolhidos aleatoriamente de modo a satisfazerem as seguintes condições:

$$\begin{aligned} & r_i \, , \; s_j \in [\; 0 \, , \, 2^r - 1 \;] \\ & q_i \, , \; p_j \in [\; 2^q \, , \, 2^{q+1} - 1 \;] \\ & u \in [\; 2^{n+r-1} \, , \, 2^{n+r} - 1 \;] \\ & v \in [\; 2^{q-2} \, , \, 2^{q-1} - 1 \;] \end{aligned} \qquad \text{(IV-60)}$$

Graficamente, tem-se :

	Número de bits no bloco					
	r	n	t	t-1	1	q
a'_i	qualquer	0...010...0 (i)	0....0	0...0	1	qualquer
b'_j	qualquer	0...000...0	0....0	0...0	1	qualquer
M	1	qualquer	0...01	0...0	0	1	qualquer

A chave de cifrar $a = (a_1,...,a_n)$ e o vetor ruído $b = (b_1,...,b_k)$ são determinados pela multiplicação modular :

$$a_i \equiv a'_i \,.\, w \bmod M \quad , \quad 1 \leq i \leq n \qquad \text{(IV-61)}$$

$$b_j \equiv b'_j \,.\, w \bmod M \quad , \quad 1 \leq j \leq k \qquad \text{(IV-62)}$$

O usuário, então, publica os (n+k) elementos obtidos: $a_1, a_2,..., a_n, b_1, b_2,..., b_k$.

No processo de cifração de uma mensagem binária, representada pelo vetor $x = (x_1,...,x_n)$ onde x_i=0 ou 1, o usuário deve, primeiramente, gerar um vetor aleatório $\ell = (\ell_1,...,\ell_k)$ onde ℓ_j=0 ou 1 (que representa o ruído), e, então, calcular o criptograma C da seguinte forma :

$$C = \sum_{i=1}^{n} x_i.a_i + \sum_{j=1}^{k} \ell_j.b_j \qquad \text{(IV-63)}$$

O usuário, então, envia ao receptor autorizado o valor do criptograma gerado.

No processo de decifração, o receptor utiliza os parâmetros secretos w e M para recuperar a mensagem a partir do criptograma recebido.

Primeiramente é executada a transformação modular inversa :

$$C' = C \cdot w^{-1} \mod M \qquad \text{(IV-64)}$$

ou ainda, usando (IV-63) :

$$C' \equiv \left(\sum_{i=1}^{n} x_i . a_i + \sum_{j=1}^{k} \ell_j . b_j \right) . w^{-1} \mod M$$

Usando as expressões (IV-61) e (IV-62) vem :

$$C' \equiv \left(\sum_{i=1}^{n} x_i . a'_i + \sum_{j=1}^{k} \ell_j . b'_j \right) . \mod M \qquad \text{(IV-65)}$$

Fazendo :

$$S = \sum_{i=1}^{n} x_i . a'_i + \sum_{j=1}^{k} \ell_j . b'_j \qquad \text{(IV-66)}$$

pode-se escrever :

$$S \leq \sum_{i=1}^{n} a'_i + \sum_{j=1}^{k} b'_j \qquad \text{(IV-67)}$$

pois, no máximo, $x_i = 1$, $1 \leq i \leq n$ e $\ell_j = 1$, $1 \leq j \leq k$.

Por construção, $a'_i < 2M$, $1 \leq i \leq n$ e $b'_j < 2M$, $1 \leq j \leq k$ (o que pode ser verificado usando o maior valor possível para a'_i e b'_j , e o menor valor para M , fornecidos pelas expressões (IV-56), (IV-57) e (IV-58) respectivamente) e, então, tem-se :

$$S < 2.(n+k).M \qquad \text{(IV-68)}$$

Consequentemente, existe um inteiro f ,satisfazendo a condição $0 \leq f \leq 2(n+k)$, tal que :

$$S - f.M = C' \qquad \text{(IV-69)}$$

pois, pelas expressões (IV-65) e (IV-66), tem-se :

$$C' = S \bmod M \qquad \text{(IV-70)}$$

Substituindo na equação (IV-66) os valores definidos em (IV-56) e (IV-57) para as variáveis a'_i e b'_j, respectivamente, e considerando o valor do módulo M dado pela equação (IV-58), então a equação (IV-69) torna-se :

$$C' = h.2^{2t+q} - f.2^{t+q} - f.v + \sum_{i=1}^{n} x_i.q_i + \sum_{j=1}^{k} \ell_j.p_j \qquad \text{(IV-71)}$$

onde:

$$h = \left(\sum_{i=1}^{n} x_i.r_i + \sum_{j=1}^{k} \ell_j.s_j \right).2^n + \sum_{i=1}^{n} x_i.2^{i-1} - f.u$$

Note-se que, usando (IV-55) e (IV-60) :

$$\sum_{i=1}^{n} x_i.q_i + \sum_{j=1}^{k} \ell_j.pj \leq \sum_{i=1}^{n} q_i + \sum_{j=1}^{k} p_j < \ldots$$

$$\ldots < (n+k).2^{q+1} \leq 2^{t+q} \qquad \text{(IV-72)}$$

Como, por construção, $a'_i \leq 2M$, $1 \leq i \leq n$ e $b'_j \leq 2M$, $1 \leq j \leq k$, então de (IV-66) vem :

$$S \leq 2.M \left(\sum_{i=1}^{n} x_i + \sum_{j=1}^{k} \ell_j \right) \qquad \text{(IV-73)}$$

Uma vez que o valor C' não pode ser negativo,

$C' \geq 0$, sendo $C' = S - f.M$,

logo:

$$S \geq f.M \qquad \text{(IV-74)}$$

Usando (IV-73) e (IV-74), pode-se escrever :

$$f.M \leq S \leq 2.M \left(\sum_{i=1}^{n} x_i + \sum_{j=1}^{k} \ell_j \right) \qquad \text{(IV-75)}$$

Assim, de (IV-75), vem :

$$f \leq 2 \left(\sum_{i=1}^{n} x_i + \sum_{j=1}^{k} \ell_j \right) \qquad \text{(IV-76)}$$

Usando o valor máximo para v , e o valor mínimo para q_i e p_j definidos em (IV-60), obtêm-se :

$$\sum_{i=1}^{n} x_i.q_i + \sum_{j=1}^{k} \ell_j.p_j - f.v \geq \ldots$$

$$\ldots \geq \left(\sum_{i=1}^{n} x_i + \sum_{j=1}^{k} \ell_j \right).2^q - f.2^{q-1} > 0 \qquad \text{(IV-77)}$$

Usando as expressões (IV-72) e (IV-77) e o fato de que C' é positivo, observa-se que o complemento-a-dois de f estará nas posições de bit t+q+1 a 2t+q da representação binária de C' . Assim, após calcular C' pela expressão (IV-64), o receptor pode, facilmente, obter o valor de f , e então determinar S usando (IV-69) . Uma vez calculado o valor S , a mensagem $x = (x_1,\ldots,x_n)$ recairá nas posições de bit 2t+q+1 a 2t+q+n da representação binária de S . (Vide exemplo a seguir)

Resumindo, o processo de decifração consiste, basicamente, de quatro etapas :

1ª - Calcular C' a partir do criptograma recebido C e dos parâmetros secretos :

$$C' = C \cdot w^{-1} \mod M$$

2ª - Determinar f a partir de C', pois o complemento-a-dois de f está nas posições de bit t+q+1 a 2t+q da representação binária de C'. (A posição t+q+1 corresponde ao bit menos significativo, e a posição 2t+q ao bit mais significativo).

3ª - Determinar S conhecidos C' , M , f :

$$S = C' + f.M$$

4ª - A partir de S, determinar a mensagem $x = (x_1,\ldots,x_n)$, binária, que recairá nas posições de bit 2t+q+1 a 2t+q+n da representação binária de S. (O elemento x_i corresponde ao bit 2t+q+i de S).

NOTA : Para determinar o complemento-a-dois de um número binário basta inverter este número (trocar os 0's por 1's e vive-versa) e somar 1(um) ao número obtido.

IV.2.2.3.2 - EXEMPLO DE APLICAÇÃO

Sejam os parâmetros :

$n = 4$, $k = 2$, $r = 2$, $q = 3$

Então podem ser calculados :

$$t = \lceil \log_2 (n+k) \rceil + 1 = \lceil \log_2 6 \rceil + 1 = 4$$

$$r_i \ , \ s_j \in [\ 0 \ , \ 2^r-1 \ ] = [\ 0 \ , \ 3 \ ]$$

$$q_i \ , \ p_j \in [\ 2^q \ , \ 2^{q+1}-1 \ ] = [\ 8 \ , \ 15 \ ]$$

$$u \in [\ 2^{n+r-1} , \ 2^{n+r}-1 \ ] = [\ 32 \ , \ 63 \ ]$$

$$v \in [\ 2^{q-2} \ , \ 2^{q-1}-1 \ ] = [\ 2 \ , \ 3 \ ] \ ,$$

sendo escolhidos os seguintes valores para as variáveis :

$r_1=2$, $r_2=3$, $r_3=1$, $r_4=0$, $s_1=2$, $s_2=1$

$q_1=10$, $q_2=8$, $q_3=11$, $q_4=13$, $p_1=9$, $p_2=15$

$u = 35$, $v = 2$

$$M = u.2^{2t+q} + 2^{t+q} + v = 35.(2^{8+3}) + 2^{4+3} + 2$$

$$M = 71810$$

Escolhendo : $w = 77$ $\therefore$ $w^{-1} = 4663 \bmod 71810$

Para $1 \leq i \leq 4$: $a'_i = r_i.2^{15} + 2^{i+10} + q_i$

Para $1 \leq j \leq 2$: $b'_j = s_j.2^{15} + p_j$

Assim, considerando os valores acima, obtém-se :

a' = (67594, 102408, 40971, 16397)

b' = (65545, 32783)

A partir desses valores podem ser calculados :

$$a_i = 77\ a'_i \mod 71810 \quad , \quad i = 1,2,3,4$$

$$b_j = 77\ b'_j \mod 71810 \quad , \quad j = 1,2$$

$$a = (34418, 58126, 66937, 41799)$$

$$b = (20265, 10941)$$

- Cifração

Sejam :

$x = (1, 0, 1, 1)$ o vetor-mensagem binário

$\ell = (0, 1)$ o vetor-ruído binário .

O criptograma a ser enviado ao receptor será :

$$C = \sum_{i=1}^{4} x_i . a_i + \sum_{j=1}^{2} \ell_j . b_j$$

$$C = (34418 + 66937 + 41799) + (10941)$$

$$C = 154095$$

- Decifração

1º - Cálculo de C'

$$C' = C \cdot w^{-1} \mod M$$

$$C' = (154095 \times 4663) \mod 71810$$

$$C' = 14125 \quad ,$$

cuja representação binária é :

$$C'_{(2)} = 11011100101101$$

2º - Determinação de f

O complemento-a-dois de f está contido na representação binária de C' , nas posições de bit t+q+1 (=8) a 2t+q (=11) , ou seja, o bit menos significativo corresponde ao 8º bit da representação binária de C' e o mais significativo ao 11º bit. Assim :

complemento-a-dois de f = 1110

Pode-se, então, determinar f :

$$f_{(2)} = (\overline{1110}) + 1 = 0001 + 1 = 0010$$

$$\therefore \quad f = 2$$

3º - Cálculo de S

$$S = C' + f.M$$

$$S = 14125 + 2 \times 71810$$

$$S = 157745 \quad ,$$

cuja representação binária é :

$$S_{(2)} = 100110100000110001$$

4º - Recuperação da mensagem

A mensagem $x = (x_1, x_2, x_3, x_4)$ está contida em S , nas posições de bit 2t+q+1 (=12) a 2t+q+n (=15) , ou seja, o elemento x_i corresponde ao bit 2t+q+i da representação binária de S . Assim :

$$x = (x_1, x_2, x_3, x_4) = (1, 0, 1, 1)$$

(Note-se que não interessa recuperar o ruído).

IV.2.2.3.3 - COMENTÁRIOS

O sistema criptográfico proposto por BRICKELL [19] , baseado no algoritmo da mochila, segue a mesma idéia básica do criptossistema de Merkle-Hellman, apresentando duas diferenças fundamentais : o módulo M não é maior que a soma dos elementos da mochila inicial fácil (o que significa que as transformações modulares não são M-dominantes), e é utilizado um vetor de ruídos para incorporar aleatoriedade ao sistema e servir como elemento complicador para a tarefa do criptoanalista.

No processo de obtenção da chave pública é utilizada uma transformação modular (não M-dominante), com parâmetros secretos w e M adequadamente escolhidos, para gerar a chave de cifrar a partir de uma seqüência fácil com estrutura bem definida. O vetor de ruídos também é gerado por um processo idêntico ao de obtenção da chave pública.

O processo de cifração da mensagem utiliza o vetor chave de cifrar e o vetor de ruídos para calcular o criptograma a ser enviado ao receptor autorizado.

A decifração do criptograma para obter a mensagem é um processo simples, utilizando a transformação modular inversa e o conceito de complemento-a-dois para determinar a variável de cuja representação binária serão extraídos os bits correspondentes da mensagem.

É evidente que o usuário do sistema criptográfico proposto por Brickell deve ficar atento à escolha de todos os parâmetros e variáveis utilizados no processo de obtenção da chave de cifrar, pois uma escolha inadequada pode implicar a geração de uma seqüência supercrescente ou com elemento dominante ou qualquer outra seqüência fácil insegura.

O ataque criptoanalítico proposto por SHAMIR [27], e também o ataque apresentado por ADLEMAN [34], ao criptossistema mochila de chave pública residem no fato de que o módulo M satisfaz a condição de dominância. No entanto, no criptossistema proposto por BRICKELL [19] tal condição não é mantida, e de fato muitos elementos da mochila fácil inicial são maiores que o módulo. Assim sendo, não parecem existir modificações simples nos ataques mencionados que possam causar sérias ameaças ao criptossistema de Brickell.

Os ataques criptoanalíticos apresentados em [35] e [43] dependem apenas do fato de que o vetor resultante (chave de cifrar) tende a ser de baixa densidade, após a multiplicação modular. Os ataques a mochilas de baixa densidade obtêm sucesso quando a densidade (D) é menor que 0,645 . Se no sistema de Brickell for escolhido, por exemplo, r=q=n-t e k=3n , então a densidade da mochila difícil resultante será D=2 . Assim sendo, escolhendo-se valores adequados para os parâmetros e variáveis utilizadas no processo de obtenção da chave pública de cifrar, é possível gerar uma mochila densa, e, desta forma, os ataques criptoanalíticos baseados na "baixa densidade", apresentados em [35] e [43], serão ineficazes.

Um tipo de ataque ao qual o sistema de Brickell talvez não consiga resistir é o ataque por reduções sucessivas, [6], [21] e [26].

IV.2.2.4 - MOCHILA "FÁCIL"

O algoritmo original proposto por MERKLE e HELLMAN [3] utiliza seqüências fáceis supercrescentes, implicando que a relação entre o último (maior) e o primeiro (menor) elemento da seqüência inicial seja grande. SHAMIR [27] se baseou neste fato para quebrar o SCMH.

Uma modificação interessante proposta por PAZ DE LIMA [47] é utilizar um sistema com seqüências fáceis não-supercrescentes, evitando que a relação a_n/a_1 seja grande, e até podendo manter esta relação constante.

Para seqüências supercrescentes a relação entre os elementos extremos cresce com o tamanho n da seqüência; segundo PAZ DE LIMA [47], para seqüências injetivas não-supercrescentes esta relação pode ser limitada e independente de n .

A seguir é apresentada a formulação proposta por PAZ DE LIMA [47].

IV.2.2.4.1 - CONCEITUAÇÃO BÁSICA

A filosofia do sistema proposto por PAZ DE LIMA [47] é determinar, a partir de uma seqüência não-supercrescente pequena (cuja solução do problema mochila associado é obtida pelo uso de tabela), uma seqüência injetiva "difícil" a ser usada como chave de cifrar no criptossistema mochila de chave pública.

O processo de obtenção da chave pública no sistema proposto em [47] começa com a escolha de uma seqüência fácil inicial pequena, tal que a relação entre o maior e o menor elemento não seja muito grande.

Esta seqüência inicial não perderá suas propriedades se for multiplicada por um número r_j qualquer. Após a multiplicação, pode-se acrescentar, ao final da seqüência, um número s_j (não múltiplo de r_j) e ainda assim continua-se com uma seqüência de fácil resolução. Este número pode ser escolhido de modo que a relação entre o maior e o menor elemento da seqüência não se altere. Este procedimento pode ser repetido até que seja obtida uma seqüência de tamanho n desejado. A esta seqüência deve ser aplicada uma transformação modular para torná-la mais segura do ponto de vista criptográfico.

O algoritmo para geração da chave pública de cifrar compreende os seguintes passos :

1º PASSO : Escolher uma seqüência fácil (injetiva) inicial de tamanho $k < n$, tal que a razão entre o maior e o menor elemento da seqüência não seja grande :

$$a^{(0)} = (a_1^{(0)}, a_2^{(0)}, \ldots, a_k^{(0)})$$

2º PASSO : Multiplicar os elementos da seqüência por um número r_j e acrescentar à seqüência obtida um número s_j, que não seja múltiplo de r_j . (Se for desejado que a relação entre o maior e o menor elemento da seqüência obtida seja igual à anterior, então o número s_j deve ser menor que o maior elemento da seqüência multiplicada e maior que o menor).

$$a^{(j)} = (a_1^{(j)}, a_2^{(j)}, \ldots, a_{k+j}^{(j)}) \quad , \quad j = 1, \ldots, n-k$$

(O 2º PASSO é repetido n-k vezes, até ser obtida a seqüência de tamanho n desejado).

3º PASSO : Aplicar uma transformação modular M-dominante, w mod M, à seqüência resultante (w e M adequadamente escolhidos) ou um multiplicador matricial (escolher uma matriz de difusão adequada) para esconder a propriedade da seqüência "fácil".
Parar o processamento.
A chave secreta é :

$$a^{(0)} = (a_1^{(0)}, a_2^{(0)}, \ldots, a_k^{(0)}) \quad ,$$

e os parâmetros secretos são :

$$(r_j , s_j , 1 \leq j \leq n-k ; w , M)$$

A chave pública de cifrar, obtida após n-k iterações é :

$$a = (a_1 , a_2 , \ldots, a_n)$$

O processo de cifração é idêntico ao do SCMH. O criptograma é obtido calculando-se o produto escalar entre a chave pública de cifrar $a = (a_1, \ldots, a_n)$ e a mensagem binária $x = (x_1, \ldots, x_n)$, da forma :

$$S = \sum_{i=1}^{n} x_i . a_i \qquad \text{(IV-78)}$$

A decifração do criptograma é feita processando-se todas as operações inversas àquelas utilizadas no processo de obtenção da chave pública de cifrar :

1º - Se tiver sido utilizada a transformação modular w mod **M**, então calcular :

$$S^{(n)} = S \, . \, w^{-1} \mod \mathbf{M} \qquad \text{(IV-79)}$$

Se $S^{(n)}$ for múltiplo de r_{n-k} , então $x_n = 0$, caso contrário $x_n = 1$.

2º - Calcular o valor do criptograma correspondente ao vetor mochila de tamanho n-1 , fazendo :

$$S^{(n-1)} = \frac{S^{(n)} - s_{n-k} \cdot x_n}{r_{n-k}} \qquad \text{(IV-80)}$$

Se $S^{(n-1)}$ for múltiplo de r_{n-k-1} , então $x_{n-1} = 0$, caso contrário $x_{n-1} = 1$.

3º - Calcular :

$$S^{(n-2)} = \frac{S^{(n-1)} - s_{n-k-1} \cdot x_{n-1}}{r_{n-k-1}} \qquad \text{(IV-81)}$$

Se $S^{(n-2)}$ for múltiplo de r_{n-k-2} , então $x_{n-2} = 0$, caso contrário $x_{n-2} = 1$.

⋮

Repetir o processo n-k vezes até ser obtido o criptograma correspondente à seqüência inicial fácil. A partir daí os k bits restantes da mensagem são determinados facilmente, pois a solução para o problema mochila associado à seqüência inicial $a^{(0)} = (a_1^{(0)}, \ldots, a_k^{(0)})$ é obtida pelo uso de uma tabela.

Desta forma a mensagem é recuperada de maneira simples, a partir do conhecimento do criptograma, da chave secreta e dos parâmetros secretos.

IV.2.2.4.2 - EXEMPLO DE APLICAÇÃO

Seja a seqüência injetiva inicial não-supercrescente :

$$a^{(0)} = (3, 5, 6, 7) \quad , \quad (k=4)$$

cuja tabela para resolução dos problemas mochila é :

Subconjunto	Soma dos elementos
$\emptyset$	0
{ 3 }	3
{ 5 }	5
{ 6 }	6
{ 7 }	7
{ 3 , 5 }	8
{ 3 , 6 }	9
{ 3 , 7 }	10
{ 5 , 6 }	11
{ 5 , 7 }	12
{ 6 , 7 }	13
{ 3 , 5 , 6 }	14
{ 3 , 5 , 7 }	15
{ 3 , 6 , 7 }	16
{ 5 , 6 , 7 }	18
{ 3 , 5 , 6 , 7 }	21

Pela tabela acima fica confirmada a propriedade da seqüência $a^{(0)}$ ser fácil, mesmo não sendo supercrescente. Observa-se, também, que a razão entre o maior e o menor elemento da seqüência não é muito grande : 7/3 .

Escolhendo $r_1 = 2$ e $s_1 = 11$, obtém-se :

$$a^{(1)} = (6, 10, 12, 14, 11)$$

Esta seqüência continua sendo fácil, e a razão entre o maior e o menor elemento não se alterou (=7/3) .

Repetindo-se o processo para :

$$r_2 = 3 \quad , \quad r_3 = 5 \quad , \quad r_4 = 4$$

$$s_2 = 13 \quad , \quad s_3 = 29 \quad , \quad s_4 = 55$$

obtêm-se, sucessivamente :

$$a^{(2)} = (18, 30, 36, 42, 33, 13)$$

$$a^{(3)} = (90, 150, 180, 210, 165, 65, 29)$$

$$a^{(4)} = (360, 600, 720, 840, 660, 260, 116, 55)$$

Aplicando à seqüência $a^{(4)}$ uma transformação modular com **M** = 3617 (> 3611) e w = 1 (w^{-1} = 1 mod 3617), (para efeito de facilidade dos cálculos), a chave de cifrar a ser publicada é a própria seqüência $a^{(4)}$:

$$a = (360, 600, 720, 840, 660, 260, 116, 55)$$

Para a mensagem binária x = (1, 0, 1, 0, 0, 1, 1, 1) de 8 bits (n=8), o criptograma correspondente será :

$$S = 360 + 720 + 260 + 116 + 55 = 1511$$

O receptor autorizado começa o processo de decifração a partir do valor **S** recebido , efetuando a transformação modular inversa :

$$S^{(8)} = (1511 \cdot w^{-1}) \cdot \text{mod } M$$

$$S^{(8)} = (1511 \times 1) \text{ mod } 3617$$

$$S^{(8)} = 1511$$

Como $S^{(8)} = 1511$ não é múltiplo de $r_4 = 4$, então:

$$x_8 = 1$$

Descontando a parcela correspondente ao bit x_8 e dividindo-se o valor obtido por $r_4 = 4$, obtém-se :

$$S^{(7)} = \frac{1511 - 55}{4} = 364$$

Como $S^{(7)} = 364$ não é múltiplo de $r_3 = 5$, então :

$$x_7 = 1$$

Repetindo-se o processo vem :

$$S^{(6)} = \frac{364 - 29}{5} = 67$$

Como $S^{(6)} = 67$ não é múltiplo de $r_2 = 3$, então :

$$x_6 = 1$$

$$S^{(5)} = \frac{67 - 13}{3} = 18$$

Como $S^{(5)} = 18$ é múltiplo de $r_1 = 2$, então :

$$x_5 = 0$$

$$S^{(4)} = \frac{18 - 0}{2} = 9$$

A partir do valor $S^{(4)} = 9$ (que corresponde à seqüência inicial) e usando a tabela , podem ser facilmente determinados os quatro bits restantes :

$$x_4 = 0 \quad , \quad x_3 = 1 \quad , \quad x_2 = 0 \quad , \quad x_1 = 1$$

Desta forma foi possível recuperar toda a mensagem :

$$x = (1, 0, 1, 0, 0, 1, 1, 1)$$

IV.2.2.4.3 - COMENTÁRIOS

O sistema criptográfico de chave pública tipo mochila proposto por PAZ DE LIMA [47] pode ser considerado como uma generalização do SCMH apresentado em [3].

Devido às suas características, o criptossistema apresentado em [47] resiste aos ataques de recuperação da informação "trapdoor" [25], [27] e [29], uma vez que não utiliza seqüência supercrescente como chave secreta e, também, a razão entre o maior e o menor elemento desta seqüência é pequena.

Ainda, o processo de obtenção da chave pública pode gerar uma mochila densa, capaz de resistir aos ataques apresentados em [35] e [43] para quebrar mochilas de baixa densidade.

O método criptográfico apresentado em [47] foi formulado com o propósito de evitar o ataque de SHAMIR [27] e similares, e desta forma nada se pode garantir quanto à resistência do método aos ataques por reduções sucessivas [6], [21] e [26].

IV.2.3 - MOCHILA UTILIZANDO NÚMEROS PRIMOS

IV.2.3.1 - INVERSO MULTIPLICATIVO

Em 1985 DI PORTO [45] propôs um algoritmo criptográfico de chave pública baseado em uma modificação do bem conhecido método criptográfico da mochila "trapdoor".

O método de Di Porto oferece maior garantia de segurança na comunicação e apresenta maior flexibilidade, permitindo a codificação de mensagens com símbolos pertencentes a um alfabeto de muitos valores.

O autor apresentou dois métodos : o método básico e o método modificado.

Em tais métodos, a chave pública consiste de n elementos que são inversos multiplicativos de números primos (método básico) ou de produto de dois números primos módulo um grande número primo M (método modificado).

A descrição dos métodos é apresentada a seguir.

IV.2.3.1.1 - CONCEITUAÇÃO BÁSICA

==== MÉTODO BÁSICO ====

Para geração da chave secreta e da chave pública, um usuário genérico A do sistema criptográfico deve executar o seguinte procedimento :

1º PASSO : Escolher, aleatoriamente, n números primos :

$$p_i > 2 \quad , \quad i = 1,2,\ldots,n$$

e calcular :

$$P = \prod_{i=1}^{n} p_i \quad ; \quad \overline{P}_i = \frac{P}{p_i} \quad , \; i=1,\ldots,n \qquad \text{(IV-82)}$$

2º PASSO : Escolher um número primo M e um inteiro a , tais que :

$$M > a \cdot \sum_{i=1}^{n} \overline{P}_i$$

$$0 < a < p_i \quad , \; i=1,\ldots,n \qquad \text{(IV-83)}$$

3º PASSO : Calcular o inverso multiplicativo de p_i módulo M , fazendo :

$$\left[\frac{1}{p_i}\right]_M = \left[\frac{(-1)^{p_i-1}\,(M-1)\,(M-2)\ldots(M-p_i+1)}{1.2\ldots p_i}\right]_M \qquad \text{(IV-84)}$$

ou aplicando outro método conhecido : [21], [60], [61], [62]

4º PASSO : Formar a chave pública [a , P(A)] , onde :

$$P(A) = \left\{ \left[\frac{1}{p_1}\right]_M , \ldots , \left[\frac{1}{p_n}\right]_M \right\}$$

Pode-se ainda modificar os elementos de P(A) somando, algebricamente, um múltiplo diferente do módulo M, a cada componente, para mascarar ainda mais os elementos do vetor.

5º PASSO : Manter secretos os números p_i , i=1,...,n e M , que determinam a chave secreta [M , S(A)], onde :

$$S(A) = (\overline{P}_1, \overline{P}_2, \ldots, \overline{P}_n)$$

No processo de cifração, um usuário B, desejando comunicar-se criptograficamente com o usuário A, efetua duas operações para formar o criptograma :

1ª - Traduzir a mensagem em uma seqüência numérica de valores compreendidos entre 0 e a , e dividir esta seqüência em blocos de n símbolos para formar vetores de n elementos :

$$X = (x_1, x_2, \ldots, x_n) \qquad 0 \leq x_i \leq a \ , \ i=1,\ldots,n$$

2ª - Cifrar a mensagem com a chave pública do destinatário desejado calculando, para cada X, o criptograma :

$$C = P(A) \ . \ X^T \qquad \text{(IV-85)}$$

Para decifrar a mensagem, o usuário A, de posse do valor recebido C, executa as seguintes operações :

1ª - Calcular :

$$C' = C \ . \ P \mod M \qquad \text{(IV-86)}$$

$$C' = S(A) \ . \ X^T$$

2ª - Recuperar, univocamente, todos os componentes x_i do vetor mensagem X resolvendo a n congruências lineares :

$$[\overline{P}_i . x_i]_{p_i} = C' \mod p_i \ , \ i=1,\ldots,n \qquad \text{(IV-87)}$$

==== MÉTODO MODIFICADO ====

Para geração da chave pública de cifrar usando o método modificado, um usuário A deve executar o seguinte procedimento :

1º PASSO : Escolher, aleatoriamente, n números primos :

$$p_i > 2 \quad , \quad i = 1,2,\ldots,n$$

e calcular :

$$P = \prod_{i=1}^{n} p_i \quad ; \quad \overline{P}_i = \frac{P}{p_i \cdot p_{i+1}} \quad , \quad i=1,\ldots,n-1 \qquad \text{(IV-88)}$$

2º PASSO : Escolher um número primo M e um inteiro a , tais que :

$$M > a \cdot \sum_{i=1}^{n-1} \overline{P}_i \qquad \text{(IV-89)}$$

$$0 < a < p_i \quad , \quad i=1,\ldots,n$$

3º PASSO : Calcular o inverso multiplicativo de $[\, p_i \cdot p_{i+1} \,]$ módulo M , i=1,2,...,n-1, e formar a chave pública que agora terá n-1 elementos :

$$P(A) = \left\{ \left[\frac{1}{p_1 p_2}\right]_M , \left[\frac{1}{p_2 p_3}\right]_M , \ldots , \left[\frac{1}{p_{n-1} p_n}\right]_M \right\}$$

Também para este caso vale a observação feita anteriormente no que se refere a somar, algebricamente , um múltiplo diferente do módulo M a cada componente do vetor P(A) antes de publicá-lo.

O processo de cifração das mensagens é idêntico ao processo descrito no Método Básico.

A decifração da mensagem é semelhante ao processo apresentado no Método Básico, com a diferença de que a recuperação dos elementos do vetor mensagem é feita de modo iterativo, resolvendo-se n-1 congruências lineares. Desta forma, o usuário A, de posse do criptograma recebido C, executa as seguintes operações :

1ª - Calcular :

$$C' = C \cdot P \mod M \qquad \text{(IV-90)}$$

2ª - Recuperar, univocamente, todos os componentes x_i do vetor-mensagem X resolvendo, iterativamente, as n-1 congruências lineares :

$$[\ \overline{P}_1 . x_1\ ]_{p_1} = [\ C'\ ]_{p_1} = C' \mod p_1 \qquad \text{(IV-91)}$$

Tem-se que : $[\ C'\ ]_{p_1} = [\ \overline{P}_1\ ]_{p_1} \cdot x_1$

porque todos os $\overline{P}_i$, $i \neq 1$, possuem p_1 como fator, logo, reduzindo-se módulo p_1 os termos em que $\overline{P}_i$ aparece para $i \neq 1$, encontrar-se-á 0(zero).

Obtido o valor x_1 , subtrai-se de C' a parcela $\overline{P}_1 . x_1$ para então recuperar x_2 :

$$[\ \overline{P}_2 . x_2\ ]_{p_2} = [\ C' - \overline{P}_1 . x_1\ ]_{p_2} \qquad \text{(IV-92)}$$

Genericamente :

$$[\ \overline{P}_{i-1} . x_{i-1} + \overline{P}_i . x_i\ ]_{p_i} = [\ C'\ ]_{p_i} = C' \mod p_i \quad , i=2,\ldots,n-1$$

ou (IV-93)

$$[\ \overline{P}_i . x_i\ ]_{p_i} = [\ C' - \overline{P}_{i-1} . x_{i-1}\ ]_{p_i} \quad , i = 2,\ldots,n-1$$

Desta forma são recuperados todos os elementos do vetor-mensagem X .

IV.2.3.1.2 - EXEMPLOS DE APLICAÇÃO

Nos exemplos a seguir são utilizados números de ordem de grandeza pequena a fim de facilitar os cálculos, uma vez que o objetivo é mostrar a técnica de utilização do algoritmo.

1º - Método Básico

Sejam os seguintes números primos:

$p_1=5$, $p_2=11$, $p_3=13$, $p_4=7$, $p_5=3$

Calculando-se :

$$P = \prod_{i=1}^{5} p_i$$

obtém-se :

$P = 5 \times 11 \times 13 \times 7 \times 3$ $\quad \therefore \quad$ $P = 15015$

Com este valor podem ser determinados, usando (IV-82):

$$\overline{P}_1 = \frac{15015}{5} = 3003$$

$$\overline{P}_2 = \frac{15015}{11} = 1365$$

$$\overline{P}_3 = \frac{15015}{13} = 1155$$

$$\overline{P}_4 = \frac{15015}{7} = 2145$$

$$\overline{P}_5 = \frac{15015}{3} = 5005$$

Chave secreta : $S(A) = (3003,1365,1155,2145,5005)$

O valor a é escolhido tal que : $0 < a < p_{i_{min}}$. Seja , então :

$$a = 2 .$$

Escolher um número primo M tal que satisfaça a equação (IV-83) :

$$M > 2 \cdot (3003+1365+1155+2145+5005)$$

$$M > 25346 \qquad \therefore \qquad M = 26731$$

A chave pública de cifrar do usuário A será :

$$P(A)_1 = [\ 1/5\ ]_M = 21385$$
$$P(A)_2 = [\ 1/11\ ]_M = 24301$$
$$P(A)_3 = [\ 1/13\ ]_M = 8225 \qquad (M = 26731)$$
$$P(A)_4 = [\ 1/7\ ]_M = 15275$$
$$P(A)_5 = [\ 1/3\ ]_M = 17821$$

$$P(A) = (21385,24301,8225,15275,17821)$$

Seja a mensagem X , em que $x_i \leq a$, $1 \leq i \leq 5$,a ser transmitida pelo usuário B ao usuário A :

$$X = (1, 0, 2, 1, 0)$$

O criptograma correspondente a este bloco de mensagem, a ser enviado ao usuário A, será :

$$C = P(A) \cdot X^T = 53110$$

O usuário A, para decifrar o criptograma, procede da seguinte maneira :

1 - Cálculo de : $C' = C \cdot P \mod M$

$$C' = (53110 \times 15015) \mod 26731$$

$$C' = 7458$$

$$C' = S(A) \cdot X^T$$

2 - Recuperação do vetor-mensagem X , a partir de C', resolvendo as congruências lineares definidas em (IV-87) , para determinar cada componente x_i :

$i=1$, $\quad [\ 3003\ x_1\ ]_5 = 7458 \bmod 5 = [\ 3\ ]_5$

$[\ 3\ x_1\ ]_5 = [\ 3\ ]_5 \qquad \therefore \qquad x_1 = 1$

$i=2$, $\quad [\ 1365\ x_2\ ]_{11} = 7458 \bmod 11 = [\ 0\ ]_{11}$

$[\ x_2\ ]_{11} = [\ 0\ ]_{11} \qquad \therefore \qquad x_2 = 0$

$i=3$, $\quad [\ 1155\ x_3\ ]_{13} = 7458 \bmod 13 = [\ 9\ ]_{13}$

$[\ 11\ x_3\ ]_{13} = [\ 9\ ]_{13}$

$[\ x_3\ ]_{13} = [\ 9/11\ ]_{13} \qquad \therefore \qquad x_3 = 2$

$i=4$, $\quad [\ 2145\ x_4\ ]_7 = 7458 \bmod 7 = [\ 3\ ]_7$

$[\ 3\ x_4\ ]_7 = [\ 3\ ]_7 \qquad \therefore \qquad x_4 = 1$

$i=5$, $\quad [\ 5005\ x_5\ ]_3 = 7458 \bmod 3 = [\ 0\ ]_3$

$[\ x_5\ ]_3 = [\ 0\ ]_3 \qquad \therefore \qquad x_5 = 0$

Desta forma foi possível recuperar todos os elementos do vetor-mensagem X :

$$X = (\ 1,\ 0,\ 2,\ 1,\ 0\ )$$

2º - Método Modificado

Sejam os seguintes números primos :

$p_1=5$, $p_2=11$, $p_3=13$, $p_4=7$, $p_5=3$, $p_6=19$

Calculando-se :

$$P = \prod_{i=1}^{6} p_i$$

obtém-se :

$P = 5 \times 11 \times 13 \times 7 \times 3 \times 19 \quad \therefore \quad P = 285285$

Com este valor podem ser determinados, usando (IV-88):

$$\overline{P}_i = \frac{P}{p_i \cdot p_{i+1}} \quad , \quad i = 1,\ldots,5$$

$\overline{P}_1 = 13 \times 7 \times 3 \times 19 = 5187$

$\overline{P}_2 = 5 \times 7 \times 3 \times 19 = 1995$

$\overline{P}_3 = 5 \times 11 \times 3 \times 19 = 3135$

$\overline{P}_4 = 5 \times 11 \times 13 \times 19 = 13585$

$\overline{P}_5 = 5 \times 11 \times 13 \times 7 = 5005$

Chave secreta : $S(A) = (5187,1995,3135,13585,5005)$

O valor a é escolhido tal que : $0 < a < p_{i_{min}}$. Seja, então :

$a = 2$.

Escolher um número primo **M** tal que satisfaça a equação (IV-89) :

$M > 2 . (5187+1995+3135+13585+5005)$

$M > 57814 \quad \therefore \quad M = 59009$

Cada elemento da chave pública P(A) pode ser obtido da seguinte forma :

$$P(A)_i = \left\{ \frac{1}{P_i \cdot P_{i+1}} \right\}_M \qquad i = 1,\ldots,5$$

Assim :

$P(A)_1 = [\ 1/55\ ]_M = 49353$

$P(A)_2 = [\ 1/143\ ]_M = 50756$

$P(A)_3 = [\ 1/91\ ]_M = 46040$ (M = 59009)

$P(A)_4 = [\ 1/21\ ]_M = 2810$

$P(A)_5 = [\ 1/57\ ]_M = 4141$

$P(A) = (\ 49353,50756,46040,2810,4141\ )$

Seja a mensagem X , em que $x_i \leq a$, $1 \leq i \leq 5$, a ser transmitida pelo usuário B ao usuário A :

$X = (\ 1, 2, 0, 2, 1\ )$

O criptograma correspondente a este bloco de mensagem, a ser enviado ao usuário A, será :

$C = P(A) \ . \ X^T = 160626$

O usuário A, para decifrar o criptograma, procede da seguinte maneira :

1 - Cálculo de : $C' = C \ . \ P \bmod M$

$C' = (\ 160626 \times 285285\ ) \bmod 59009$

$C' = 41352$

2 - Recuperação do vetor-mensagem X , a partir de C', resolvendo as congruências lineares definidas em (IV-91) e (IV-93), para determinar cada componente x_i :

i=1 , $[\ 5187\ x_1\ ]_5 = [\ 41352\ ]_5$

$[\ 2\ x_1\ ]_5 = [\ 2\ ]_5 \quad \therefore \quad x_1 = 1$

i=2 , $[\ 1995\ x_2\ ]_{11} = [\ 41352 - 5187\ ]_{11}$

$[\ 4\ x_2\ ]_{11} = [\ 8\ ]_{11} \quad \therefore \quad x_2 = 2$

i=3 , $[\ 3135\ x_3\ ]_{13} = [\ 41352 - (1995 \times 2)\ ]_{13}$

$[\ 2\ x_3\ ]_{13} = [\ 0\ ]_{13} \quad \therefore \quad x_3 = 0$

i=4 , $[\ 13585\ x_4\ ]_7 = [\ 41352 - (3135 \times 0)\ ]_7$

$[\ 5\ x_4\ ]_7 = [\ 3\ ]_7$

$[\ x_4\ ]_7 = [\ 3 \times (1/5)\ ]_7 = [\ 3 \times 3\ ]_7$

$[\ x_4\ ]_7 = [\ 9\ ]_7 = [\ 2\ ]_7 \quad \therefore \quad x_4 = 2$

i=5 , $[\ 5005\ x_5\ ]_3 = [\ 41352 - (13585 \times 2)\ ]_3$

$[\ x_5\ ]_3 = [\ 1\ ]_3 \quad \therefore \quad x_5 = 1$

Desta forma foi possível recuperar todos os elementos do vetor-mensagem X :

$$X = (\ 1,\ 2,\ 0,\ 2,\ 1)$$

Para diminuir a expansão de dados no processo de cifração, pode-se utilizar uma forma equivalente para a chave pública de cifrar , P(A) , considerando números menores para seus elementos.

Subtraindo-se o valor M = 59009 dos três primeiros elementos da chave pública P(A), obtém-se a forma equivalente P(A)' :

$$P(A)' = (-9656, -8253, -12969, 2810, 4141)$$

Neste caso, a cifração do bloco da mensagem :

$$X = (1, 2, 0, 2, 1)$$

fornecerá o seguinte criptograma :

$$C = P(A)' . X^T$$

$$C = - 16401$$

No processo de decifração, o usuário A calcula :

$$C' = C . P \bmod M$$

$$C' = (-16401 \times 285285) \bmod 59009$$

$$C' = 41352$$

que é o mesmo valor obtido quando foi empregada a forma original da chave pública P(A).

A partir daí o processo é idêntico.

IV.2.3.1.3 - COMENTÁRIOS

O método proposto por DI PORTO [45] apresenta uma forma original (diferente) para gerar o vetor chave pública, presumivelmente difícil, para o sistema criptográfico tipo mochila, baseando-se na Teoria dos Números (mais especificamente na dificuldade de fatoração de produto de primos).

Comparando-se o sistema mochila tradicional, proposto por MERKLE e HELLMAN [3], com o algoritmo apresentado em [45], observa-se que este último apresenta duas vantagens básicas :

- Possibilidade de cifrar mensagens pertencentes a um alfabeto de muitos símbolos (alfabeto não-binário), permitindo maior flexibilidade do conjunto de mensagens ;

- Aumento da segurança criptográfica em virtude da dificuldade de fatoração dos elementos da chave pública (produto de primos, no Método Modificado).

Como desvantagens deste algoritmo podem ser citadas as seguintes :

- O processo de decifração executa uma série de operações complexas, que são complicadas ainda mais com o emprego de números primos muito elevados exigidos para se obter um grau satisfatório de segurança ;

- Elevado grau de expansão de dados no processo de cifração. (Esta desvantagem pode ser minorada somando-se, algebricamente, múltiplos do módulo **M** a alguns elementos da chave pública, de modo a obter-se uma forma equivalente para esta chave, com elementos de menor valor absoluto. Assim, consegue-se diminuir a redundância no momento da cifração da mensagem).

A maior resistência criptográfica do Método Modificado, em relação ao Método Básico, reside na dificuldade de fatoração do produto de primos, cujo inverso multiplicativo módulo M é usado para formar um dos elementos da chave pública.

Vale ressaltar que o processo de obtenção da chave pública não está imune a gerar uma chave supercrescente. Por isso, o usuário deve ficar atento à escolha dos parâmetros geradores da chave pública, de modo que o vetor resultante seja difícil de ser resolvido.

Uma sugetão interessante, aqui apresentada, para tornar o sistema de Di Porto mais flexível, é utilizar um valor limite diferente para cada componente do vetor-mensagem :

$$0 < a_i < p_i \quad , \quad i = 1,2,\ldots,n$$

permitindo maior flexibilidade para o conjunto de mensagens, uma vez que não se limitariam pelo menor valor p_i os componentes do vetor-mensagem. Neste caso, então : $M > \sum_{i=1}^{n-1} a_i . \bar{P}_i$.

Quanto à segurança de método proposto por DI PORTO[45], pode-se afirmar que os ataques de recuperação da informação "trapdoor" [25], [27] e [29], não podem ser aplicados, uma vez que a chave pública não é obtida a partir de seqüência supercrescente usando transformações modulares.

Os ataques a mochilas de baixa densidade [35] e [43] podem não obter sucesso se, na fase de construção do sistema , forem escolhidos, por tentativa e erro, números primos e módulo M de tal forma que a chave pública gerada seja uma mochila densa.

Nada se pode garantir quanto à resistência do método de Di Porto aos ataques por reduções sucessivas [6], [21] e [26], porque este método não foi formulado com a intenção explícita de resistir a esses ataques.

IV.2.3.2 - MULTIPLICADOR MATRICIAL

Em 1984 PAZ DE LIMA [53] propôs uma outra generalização para o criptossistema mochila de chave pública.

O método criptográfico apresentado em [53] utiliza, no processo de geração da chave pública de cifrar, produto de primos para compor os elementos do vetor mochila "fácil" e uma matriz , não necessariamente invertível, usada como multiplicador desta seqüência "fácil".

O método proposto por PAZ DE LIMA se baseia na Teoria do Números (mais especificamente na dificuldade de fatoração do produto de primos) para melhorar a segurança criptográfica.

A descrição do método é apresentada a seguir.

IV.2.3.2.1 - CONCEITUAÇÃO BÁSICA

No sistema criptográfico proposto por PAZ DE LIMA [53], um usuário A, para gerar a sua chave pública de cifrar, deve executar o seguinte procedimento :

1º PASSO : Escolher, aleatoriamente, m números primos :

$$p_i > 2 \quad , \qquad i = 1,2,\ldots,m$$

e calcular :

$$P = \prod_{i=1}^{m} p_i \quad ; \quad \overline{P}_i = \frac{P}{p_i} \quad , \; i=1,\ldots,m \qquad \text{(IV-94)}$$

2º PASSO : Construir a matriz **M** , que não precisa ser quadrada nem ser invertível, de dimensão n x m , tal que:

$$\sum_{i=1}^{n} M_{ij} < p_j \quad , \quad j = 1,\ldots,m \qquad \text{(IV-95)}$$

isto é, a soma dos elementos da j-ésima coluna da matriz **M** tem que ser menor que p_j.
A matriz M deve ser construída de forma que suas colunas sejam seqüências difíceis, mas que alguma combinação linear delas seja uma seqüência "fácil" (até mesmo supercrescente).

3º PASSO : Formar o vetor mochila fácil, que é a chave secreta, com m elementos :

$$S(A) = (\overline{P}_1, \overline{P}_2, \ldots, \overline{P}_m)$$

4º PASSO : Obter a chave pública de cifrar P(A), que possui n elementos :

$$P(A)^T = M \cdot (S(A))^T \qquad \text{(IV-96)}$$

onde : M é a matriz n x m ;

S(A) é a chave secreta com m elementos.

No processo de cifração, um usuário B, que deseja se comunicar com o usuário A, deve efetuar as seguintes etapas para formar o criptograma :

1ª - Traduzir a mensagem em uma seqüência binária, dividindo-a em blocos de n elementos para formar os vetores-mensagem :

$$X = (x_1, x_2, \ldots, x_n)$$

$$x_i = 0 \text{ ou } 1 \quad , \quad i = 1, \ldots, n$$

2ª - Cifrar a mensagem com a chave pública do destinatário A , calculando o criptograma C a ser transmitido :

$$C = P(A) \cdot X^T \qquad \text{(IV-97)}$$

Para decifrar a mensagem, o usuário A, de posse do criptograma recebido C, deve executar as seguintes operações :

1ª - Calcular :

$$C \pmod{p_i} = [(X.M^{(i)}).\overline{P}_i] \bmod p_i \quad , \quad i=1,\ldots,m \qquad \text{(IV-98)}$$

onde : $M^{(i)}$ é o i-ésimo vetor-coluna da matriz M .

A expressão (IV-98) é válida porque $\overline{P}_j \bmod p_i = 0$ para $j \neq i$.

Determinar os valores $(X.M^{(i)})$, $i = 1,\ldots,m$:

$$(X.M^{(i)}) \bmod p_i = [\ 1/\overline{P}_i\ ]_{p_i} \ .\ C \ (\bmod p_i) \qquad \text{(IV-99)}$$

onde : $[\ 1/\overline{P}_i\ ]_{p_i}$ é o inverso de $\overline{P}_i$ módulo p_i .

2ª - Usar a combinação linear que gera a seqüência fácil (ou supercrescente), para recuperar os elementos do vetor-mensagem $X = (x_1, x_2, \ldots, x_n)$. Os coeficientes k_i , nulos, positivos ou negativos, que definem a combinação linear, são mantidos secretos. Assim :

$$X.[\ k_1.M^{(1)} + k_2.M^{(2)} + \ldots + k_m.M^{(m)}\ ] = \ldots$$

$$\ldots = k_1.[\ (X.M^{(1)}) \bmod p_1\ ] +$$

$$+ k_2.[\ (X.M^{(2)}) \bmod p_2\ ] + \ldots$$

$$\ldots + k_m.[\ (X.M^{(m)}) \bmod p_m\ ] \qquad \text{(IV-100)}$$

Como a seqüência que multiplica o vetor X é "fácil", e também são conhecidos todos os termos do lado direito da equação (IV-100), então a recuperação da mensagem torna-se trivial.

Vale ressaltar que a segurança criptográfica do método apresentado acima está fundamentada tanto na dificuldade de fatoração de inteiros, que são produto de números primos , como na dificuldade inerente do problema mochila . Também, a matriz usada como multiplicador da chave secreta incorpora uma dificuldade adicional na tarefa do interceptador, negando a ele informações sobre o sistema.

IV.2.3.2.2 - EXEMPLO DE APLICAÇÃO

Para ilustrar o método descrito acima, segue o exemplo numérico.

Sejam : $m = n = 4$, e os números primos :

$$p_1=41 \quad , \quad p_2=43 \quad , \quad p_3=47 \quad , \quad p_4=53$$

Usando a equação (IV-94) podem ser determinados :

$$P = 41 \times 43 \times 47 \times 53$$

$$P = 4391633$$

$$\overline{P}_1 = 107113$$

$$\overline{P}_2 = 102131$$

$$\overline{P}_3 = 93439$$

$$\overline{P}_4 = 82861$$

Desta forma, a chave secreta do usuário A é :

$$S(A) = (107113, 102131, 93439, 82861) \quad ,$$

que é uma seqüência fácil pela própria característica dos seus elementos $\overline{P}_i$, que são produto de números primos.

Seja considerada a matriz **M** de dimensão 4 x 4, que é mantida secreta :

$$M = \begin{bmatrix} 2 & 4 & 6 & 7 \\ 4 & 7 & 0 & 2 \\ 7 & 11 & 8 & 1 \\ 11 & 15 & 2 & 3 \end{bmatrix}$$

onde a soma dos elementos da i-ésima coluna é menor que p_i .

$$2 + 4 + 7 + 11 < 41$$
$$4 + 7 + 11 + 15 < 43$$
$$6 + 0 + 8 + 2 < 47$$
$$7 + 2 + 1 + 3 < 53$$

Escolhendo-se os números $k_1=3$, $k_2=-1$, $k_3=k_4=0$, pode ser definida a combinação linear das colunas da matriz **M** de forma que a seqüência obtida é supercrescente :

$$3.M^{(1)} - M^{(2)} = 3 \times \begin{bmatrix} 2 \\ 4 \\ 7 \\ 11 \end{bmatrix} - \begin{bmatrix} 4 \\ 7 \\ 11 \\ 15 \end{bmatrix} = \begin{bmatrix} 2 \\ 5 \\ 10 \\ 18 \end{bmatrix}$$

onde $M^{(i)}$ é o i-ésimo vetor-coluna da matriz M .

A chave pública de cifrar do usuário A é obtida da forma :

$$P(A)^T = M \cdot S(A)^T \quad ,$$

que fornece, para os valores acima :

$$P(A)^T = \begin{bmatrix} 1763411 \\ 1309091 \\ 2703605 \\ 3145669 \end{bmatrix}$$

Considerando o primeiro bloco da mensagem como a seqüência binária de n=4 bits :

$$X = (1, 1, 0, 1) \quad ,$$

o criptograma correspondente, a ser enviado ao usuário A , é calculado da seguinte forma :

$$C = X \cdot P(A)^T \quad , \quad \text{obtendo-se :}$$

$$C = 6218171$$

Para decifrar o criptograma recebido C , o usuário A procede da seguinte forma :

1 - Calcular, usando a expressão (IV-98) :

$$C \pmod{p_i} = [\ (X.M^{(i)}).\overline{P}_i\ ] \bmod p_i \quad , \quad i=1,2,3,4$$

ou :

$$[\ C\ ]_{p_i} = [\ (X.M^{(i)})\ ]_{p_i} \ .\ [\ \overline{P}_i\ ]_{p_i}$$

Como somente $M^{(1)}$ e $M^{(2)}$ foram usadas na combinação linear, basta calcular o valor acima par i=1 e i=2 :

i=1 ,
$$[\ (X.M^{(1)})\ ]_{41} \ .\ [\ 107113\ ]_{41} = [\ 6218171\ ]_{41}$$
$$[\ (X.M^{(1)})\ ]_{41} \ .\ [\ 21\ ]_{41} = [\ 29\ ]_{41}$$
$$[\ (X.M^{(1)})\ ]_{41} = [\ 29/21\ ]_{41} = [\ 17\ ]_{41}$$

i=2 ,
$$[\ (X.M^{(2)})\ ]_{43} \ .\ [\ 102131\ ]_{43} = [\ 6218171\ ]_{43}$$
$$[\ (X.M^{(2)})\ ]_{43} \ .\ [\ 6\ ]_{43} = [\ 27\ ]_{43}$$
$$[\ (X.M^{(2)})\ ]_{43} = [\ 27/6\ ]_{43} = [\ 26\ ]_{43}$$

2 - Usar a combinação linear definida pelos inteiros $k_1=3$, $k_2=-1$, $k_3=k_4=0$ para determinar o vetor-mensagem , conforme (IV-100):

$$X\ [\ 3.M^{(1)} - M^{(2)}\ ] = 3.[\ (X.M^{(1)})\ ]_{41} - [\ (X.M^{(2)})\ ]_{43}$$

$$X\ .\ [\ 2,\ 5,\ 10,\ 18\ ]^T = (\ 3 \times 17\ ) - 26$$

$$X\ .\ [\ 2,\ 5,\ 10,\ 18\ ]^T \equiv 25$$

Uma vez que o vetor que multiplica o vetor-mensagem X é supercrescente, torna-se trivial a obtenção da solução :

$$X = (\ 1,\ 1,\ 0,\ 1\ )$$

Desta forma foi possível recuperar a mensagem transmitida.

IV.2.3.2.3 - COMENTÁRIOS

O método proposto por PAZ DE LIMA [53] é uma generalização para o SCMH. A formulação do método é boa e simples, sendo, em alguns aspectos, similar ao Método Básico proposto por DI PORTO [45].

O processo de geração da chave pública de cifrar utiliza produto de primos para compor a mochila fácil inicial e opera a multiplicação matricial para obter os elementos da chave pública. A utilização da matriz serve para "esconder" a propriedade do vetor fácil e permitir a volta única, isto é, a recuperação da mensagem. A matriz M não precisa ter inversa e pode ser retangular, o que torna o algoritmo mais geral e, ao mesmo tempo, nega informações ao adversário. As colunas desta matriz são seqüências que não precisam ter solução (não precisam ser injetivas), mas deve existir uma combinação linear dessas colunas que gere uma seqüência fácil (ou até supercrescente) que admite solução única.

A segurança criptográfica do método é melhorada pela dificuldade de fatoração de inteiros que são produto de números primos, e também na dificuldade adicional introduzida com a utilização da matriz M (além da dificuldade inerente do problema mochila).

Os ataques de recuperação da informação "trapdoor", [25], [27] e [29], não se aplicam ao sistema apresentado em [53], pois a chave pública não é gerada a partir de seqüência supercrescente e nem são usadas transformações modulares.

Apesar de não ter sido preparado para isso, o algoritmo pode gerar mochilas densas com uma escolha apropriada dos números primos p_i e da matriz M, e neste caso os ataques a mochilas de baixa densidade, [35] e [43], podem ser evitados.

A construção do método descrito acima não garante resistência aos ataques criptoanalíticos por reduções sucessivas [6], [21] e [26].

IV.2.3.3 - REPRESENTAÇÃO MODULAR E RADIAL

Em 1985 GOODMAN e McAULEY [44] propuseram um novo criptossistema de chave pública tipo mochila "trapdoor".

Neste novo sistema, a equação de cifrar corresponde à equação geral modular da mochila, mas, diferentemente do SCMH, os componentes da mochila inicial não precisam ter estrutura supercrescente; a informação "trapdoor" é baseada nas transformações entre a forma modular e a forma radial dos componentes da mochila, usando o Teorema Chinês do Resto.

Outras características apresentadas por este sistema são :

- possibilidade de cifrar mensagens não-binárias ;
- capacidade de gerar mochila de alta densidade, pela escolha apropriada dos parâmetros ;
- expansão de dados reduzida (aproximadamente 30%) ;
- tamanho da chave pública da ordem de 14 Kbits ;
- admite a incorporação de ruído ;
- alta velocidade de cifração e decifração .

A descrição detalhada do sistema criptográfico é apresentada a seguir.

IV.2.3.3.1 - CONCEITUAÇÃO BÁSICA

Na apresentação do sistema criptográfico proposto por GOODMAN e McAULEY [44] serão utilizados os seguintes símbolos:

a_i = componente do vetor mochila público

a'_i = componente do vetor mochila secreto

a = $(a_1,\ldots,a_n)$ = vetor mochila público

a' = $(a'_1,\ldots,a'_n)$ = vetor mochila secreto

A' = matriz mochila secreta que corresponde à representação modular do vetor a'

$a_j^{(i)}$ = $a_j \bmod p_i$ = resíduo do j-ésimo componente da mochila módulo o i-ésimo primo

D = densidade do criptossistema

g = número de bits em $x_{i_{máx}}$ (coordenada máxima do vetor-mensagem x), sub-blocos da mensagem

h = número de bits em $p_{i_{mín}}$ (menor número primo p_i)

n = número de componentes da mochila; também o número de primos p_i escolhidos

p_i = i-ésimo número primo escolhido

P = $\prod_{i=1}^{n} p_i$ = produto dos n primos distintos escolhidos

PK = número de bits na chave pública

r = número de bits em $\left\{ \sum_{j=1}^{n} a_j^{'(i)} \right\}_{máx}$ $\quad i=1,\ldots,n$

S = $\sum_{i=1}^{n} a_i . x_i \bmod P$ = criptograma

S' = $S \cdot w^{-1} \bmod P$ = criptograma transformado
Na forma modular é o vetor $(S'^{(1)},\ldots,S'^{(n)})$

w = multiplicador modular secreto, sendo : $(w, P) = 1$

x = $(x_1,\ldots,x_n)$ = vetor-mensagem

A equação geral modular da mochila é dada por :

$$S = \sum_{i=1}^{n} a_i . x_i \mod P \qquad \text{(IV-101)}$$

Quando usada para fins criptográficos, os elementos a_i são os n componentes da mochila pública, P é o módulo público e os elementos x_i são componentes do vetor-mensagem. Em uma mochila binária os elementos x_i são 0 ou 1 , mas em uma mochila geral são números de até g bits. O subconjunto soma S é o criptograma, que é enviado ao usuário legítimo, a partir do qual pode ser recuperado o vetor $x = (x_1,...,x_n)$.

Seja $\{ p_1, p_2,..., p_n \}$ um conjunto de n primos, e :

$$P = \prod_{i=1}^{n} p_i \qquad \text{(IV-102)}$$

$$\overline{P}_i = \frac{P}{p_i} \quad , \quad i = 1,...,n \qquad \text{(IV-103)}$$

sendo $(\overline{P}_i)^{-1}$ o inverso multiplicativo de $\overline{P}_i$ módulo p_i .

Sejam definidas as formas de representação :

$$\text{Modular:} \quad a_j^{(i)} = a_j \mod p_i \qquad \text{(IV-104)}$$

$$\text{Radial:} \quad a_j = \sum_{i=1}^{n} a_j^{(i)} . \overline{P}_i . (\overline{P}_i)^{-1} \qquad \text{(IV-105)}$$

Então, pelo Teorema Chinês do Resto,

$$a_j \leftrightarrow a_j^{(1)} , a_j^{(2)} ,..., a_j^{(n)}$$

é uma representação bijetiva. Isto é, a transformação é bijetora para todos os elementos a_j compreendidos entre 1 e P-1.

Assim, se a fatoração de P for mantida secreta, espera-se que somente o usuário autorizado seja capaz de transformar a representação radial (escalar) dos componentes da mochila na sua representação modular (vetorial). Isso constitui a informação "trapdoor".

Seja escolhido um conjunto de n componentes mochila, cujas forma radial e modular são, respectivamente :

$$a' = \begin{matrix} a'_1 \leftrightarrow a'^{(1)}_1, a'^{(2)}_1, \ldots, a'^{(n)}_1 \\ a'_2 \leftrightarrow a'^{(1)}_2, a'^{(2)}_2, \ldots, a'^{(n)}_2 \\ \vdots \qquad\qquad \vdots \\ a'_n \leftrightarrow a'^{(1)}_n, a'^{(2)}_n, \ldots, a'^{(n)}_n \end{matrix} = A'$$

Para esconder a informação "trapdoor", utiliza-se a multiplicação modular para formar um novo conjunto de componentes mochila :

$$a_j = a'_j \cdot w \mod P \qquad \text{(IV-106)}$$

onde w e P são primos entre si. É definido como w^{-1} o inverso multiplicativo de w módulo P.

O vetor mochila $a = (a_1, a_2, \ldots, a_n)$ é a chave de cifrar, que é publicada juntamente com o módulo P .

A fatoração de P e o inteiro w são mantidos secretos, e, por conseguinte, é mantida secreta a representação modular do vetor a' (que é a matriz A').

Sejam, ainda, feitas as seguintes considerações :

$$p_{i_{mín}} \geq 2^h \qquad \text{(IV-107)}$$

isto é, os números primos possuem, no mínimo, h+1 bits.

Também :

$$x_{i_{máx}} < 2^g \qquad \text{(IV-108)}$$

isto é, os elementos da mensagem são números de, no máximo, g bits.

Ainda :

$$\left\{ \sum_{j=1}^{n} a'^{(i)}_j \right\}_{\text{máx } i} < 2^r \quad , \quad i=1,\ldots,n \qquad \text{(IV-109)}$$

isto é, o máximo das somas dos elementos das colunas de A' é um número de, no máximo, r bits.

A fim de assegurar que a equação de cifração tenha uma única decifração, deve-se garantir que a transformação da mensagem para o criptograma, $x \rightarrow S$, seja injetiva. Para garantir isso, é preciso que :

$$h \geq r + g \qquad \text{(IV-110)}$$

A condição expressa em (IV-110) também assegura que a multiplicação modular é equivalente à multiplicação matricial:

$$(S'^{(1)},\ldots,S'^{(n)}) = (x_1,\ldots,x_n) \cdot \begin{Bmatrix} a'^{(1)}_1,\ldots,a'^{(n)}_1 \\ \vdots \\ a'^{(1)}_n,\ldots,a'^{(n)}_n \end{Bmatrix} \qquad \text{(IV-111)}$$

isto é :

$$S' = x \cdot A' \quad ,$$

e que a transformação pode ser invertida (desde que a matriz A' seja não-singular) conforme :

$$x = S' \cdot (A')^{-1} \qquad \text{(IV-112)}$$

O criptossistema, então, funciona da seguinte forma:

Um usuário, para formar o criptograma correspondente à mensagem a ser transmitida, utiliza a chave pública do destinatário e calcula :

$$S = (x_1.a_1 + x_2.a_2 + \ldots + x_n.a_n) \bmod P$$

conforme a equação (IV-101).

O receptor do criptograma deverá, então, calcular S' :

$$S' = S \cdot w^{-1} \bmod P \qquad \text{(IV-113)}$$

e expressar este valor na forma modular usando a fatoração de P conhecida apenas por ele :

$$S' \leftrightarrow (S'^{(1)}, S'^{(2)}, \ldots, S'^{(n)})$$

onde : $$S'^{(i)} = S' \bmod p_i \qquad \text{(IV-114)}$$

e, então, calcular :

$$x = S' \cdot (A')^{-1}$$

conforme a equação (IV-112).

Desta forma é recuperada a mensagem em texto claro.

Deve-se notar que o criptoanalista deverá "quebrar" P para descobrir seus fatores, ou atacar a mochila "trapdoor" de uma outra maneira.

Para obter-se um criptossistema prático seguro, deve-se escolher adequadamente os valores dos parâmetros n , r , g , h .

GOODMAN e McAULEY [44] realizaram uma análise detalhada, quanto aos valores típicos para estas variáveis, considerando várias restrições de ordem prática. Ao final da análise foram estabelecidos os seguintes valores :

$n = 7$

$r = 7$

$g = 248$

$h = 255$

Para estes valores são determinados :

- Tamanho do bloco da mensagem

$$n \cdot g = 7 \times 248 = 1736 \text{ bits}$$

- Tamanho da chave pública

$$PK = n \cdot (n+1) \cdot (h+1) \text{ bits}$$

$$PK = 7 \times (7+1) \times (255+1)$$

$$PK = 14336 \text{ bits}$$

- Densidade do sistema

$$D = \frac{g}{h + 1} = \frac{248}{255 + 1} \cong 0,97$$

Para ilustrar o método descrito acima, segue um exemplo numérico simples.

IV.2.3.3.2 - EXEMPLO DE APLICAÇÃO

Sejam : $n = 3$, $g = 2$,

$p_1=37$, $p_2=41$, $p_3=43$.

Desta forma ficam determinados :

$P = 65231$, pela equação (IV-102)

$h = 5$, pela equação (IV-107)

$r = 3$, pela equação (IV-110)

Escolhendo os três elementos da mochila de modo a satisfazer a equação (IV-109), isto é, as colunas da matriz A' devem somar menos que 8 , e exprimindo esses valores nas formas modular e radial, usando (IV-105), vem :

$$A' = \begin{array}{lll} (3, 1, 1) & \leftrightarrow & 125174 = a'_1 \\ (1, 5, 3) & \leftrightarrow & 151664 = a'_2 = a' \\ (2, 1, 2) & \leftrightarrow & 122509 = a'_3 \end{array}$$

Escolhendo :

$w = 6553$,

vem:

$w^{-1} = 2618 \mod 65231$.

Executando a multiplicação modular definida pela equação (IV-106) obtém-se a chave de cifrar :

$a_1 = 50628$

$a_2 = 59907$

$a_3 = 3560$

$a = (50628, 59907, 3560)$,

que é publicada juntamente com o valor $P = 65231$.

(Observe-se que o vetor $a = (a_1, a_2, a_3)$ é supercrescente permutado, indicando que a escolha dos parâmetros não foi adequada; deve-se ficar atento a este tipo de ocorrência, a fim de evitá-la.)

A matriz $(A')^{-1}$, que é a chave de decifrar, vale :

$$(A')^{-1} = 1/16 \cdot \begin{bmatrix} 7 & -1 & -2 \\ 4 & 4 & -8 \\ -9 & -1 & 14 \end{bmatrix}$$

Para transmitir uma mensagem de 6 bits (= n x g = 2 x 3)

$$x = (1, 2, 3)$$

o usuário calcula o criptograma, usando a equação (IV-101), :

$$S = (1 \times 50628)+(2 \times 59907)+(3 \times 3560) \bmod 65231$$

$$S = 50660 \bmod 65231$$

Usando o valor secreto w^{-1}, o receptor pode calcular:

$$S' = (50660 \times 2618) \bmod 65231$$

$$S' = 13257 \bmod 65231 \quad ,$$

e conhecendo o conjunto secreto de primos { 37, 41, 43 } ,pode obter a forma modular do número S' :

$$S' = (11, 14, 13) \leftrightarrow 13257$$

Pela equação (IV-112), o receptor pode determinar :

$$x = (11, 14, 13) \cdot 1/16 \begin{bmatrix} 7 & -1 & -2 \\ 4 & 4 & -8 \\ -9 & -1 & 14 \end{bmatrix} ,$$

obtendo :

$$x = (1, 2, 3)$$

IV.2.3.3.3 - COMENTÁRIOS

O método criptográfico proposto por GOODMAN e McAULEY [44] é uma generalização para o SCMH.

Sua formulação é baseada no problema geral da mochila modular, e a informação "trapdoor" consiste nas transformações entre a forma modular e a forma radial dos componentes da mochila, usando o Teorema Chinês do Resto.

A segurança deste sistema não é fundamentada na transformação modular de uma seqüência supercrescente (como no esquema de Merkle-Hellman), mas sim na dificuldade de fatorar um inteiro que é produto de sete primos de 256 bits cada um.

As características principais apresentadas pelo método proposto são :

- os componentes da mochila inicial não precisam ter estrutura supercrescente ;
- a informação "trapdoor" consiste na representação modular e radial dos elementos da mochila ;
- segurança baseada na dificuldade de fatorar um inteiro que é produto de primos, e também no fato do problema mochila ser NP-completo ;
- possibilidade de cifrar mensagens não-binárias ;
- admite incorporar ruído na mensagem para aumentar a segurança ;
- nível de expansão de dados igual a, aproximadamente, 30%, que pode ser considerado pequeno quando comparado com 100% de expansão de dados gerada no SCMH ;
- tamanho da chave pública da ordem de 14 Kbits, que não é excessivo quando comparado com os 80 Kbits do SCMH e 1 Kbit do esquema RSA ;
- escolha adequada dos valores das variáveis permite gerar uma mochila densa, com um valor típico para a densidade de 0,97 e um bloco de mensagem de tamanho 1736 bits ;

- alta velocidade, pois a própria natureza do sistema implica que os processos de cifração e de decifração sejam rápidos quando comparados com o criptossistema RSA.

O usuário do sistema criptográfico acima descrito deve ficar atento à escolha dos valores das variáveis utilizadas no processo de obtenção da chave pública, a fim de evitar que seja gerada uma mochila de fácil solução (como, por exemplo, mochila supercrescente ou com elemento dominante).

Quanto à segurança criptográfica, pode-se afirmar que o sistema de GOODMAN e McAULEY [44] resiste aos ataques de recuperação da informação "trapdoor",[25], [27] e [29], porque não utiliza seqüência supercrescente para formação da chave pública.

Este sistema criptográfico também resiste aos ataques a mochilas de baixa densidade [35] e [43], uma vez que o algoritmo permite gerar mochilas densas com a escolha adequada dos parâmetros (conforme mostrado em [44]).

Nada pode ser garantido quanto à resistência do método proposto aos ataques por reduções sucessivas [6],[21] e [26].

IV.2.3.4 - ELEMENTOS IDEMPOTENTES

Em 1985 PIEPRZYK e RUTKOWSKI [42] propuseram uma modificação para os criptossistemas mochila de chave pública . O sistema criptográfico proposto utiliza elementos idempotentes, e pode ser considerado como uma generalização do esquema de MERKLE e HELLMAN [3].

Antes de apresentar a formulação deste sistema, serão mostrados alguns conceitos e propriedades dos elementos idempotentes.

Seja Z_N o anel dos inteiros não-negativos com adição e multiplicação módulo N , onde :

$$N = N_1 \, x \ldots x \, N_t \quad e \quad N_i = (p_i)^{\alpha_i} \quad , \; i=1,\ldots,t \qquad \text{(IV-115)}$$

sendo p_i números primos ($p_i \neq p_j$ para $i \neq j$) e $\alpha_i = 1,2,\ldots$

Assim, cada inteiro $x \in Z_N$ pode ser escrito da seguinte forma :

$$\begin{aligned} x &= [\, x(\text{mod } N_1), \ldots, x(\text{mod } N_t) \,] \\ &= [\, x_1 \, , \, x_2 \, , \ldots , \, x_t \,] \in \bigoplus_{i=1}^{t} Z_{N_i} \end{aligned} \qquad \text{(IV-116)}$$

onde $x_i \in Z_{N_i}$ ($i=1,\ldots,t$) e o anel $\bigoplus_{i=1}^{t} Z_{N_i}$ consiste de todos os elementos do anel Z_N e esta representação é bijetora ("one-to-one").

Desta forma os anéis Z_N e $\bigoplus_{i=1}^{t} Z_{N_i}$ são isomórficos e o isomorfismo g é definido como :

$$g \, [\, x(\text{mod } N) \,] = [\, x_1, \ldots, x_t \,] \in \bigoplus_{i=1}^{t} Z_{N_i} \qquad \text{(IV-117)}$$

Sejam dois elementos x , $y \in Z_N$, onde são definidos $x = [\, x_1,\ldots,x_t \,]$, $y = [\, y_1,\ldots,y_t \,]$. As operações aritméticas podem ser descritas pelas expressões :

$$\begin{aligned} x + y \,(\mathrm{mod}\ N) &= [\ (x+y) \bmod N_1,\ldots,\ (x+y) \bmod N_t\ ] \\ x + y \,(\mathrm{mod}\ N) &= [\ (x_1+y_1),\ (x_2+y_2),\ldots,\ (x_t+y_t)\ ] \end{aligned} \tag{IV-118}$$

e

$$\begin{aligned} x \,.\, y \,(\mathrm{mod}\ N) &= [\ (x.y) \bmod N_1\ ,\ldots,\ (x.y) \bmod N_t\ ] \\ x\ y\ (\mathrm{mod}\ N) &= [\ (x_1.y_1),\ (x_2.y_2),\ldots,\ (x_t.y_t)\ ] \end{aligned} \tag{IV-119}$$

Sejam considerados os seguintes vetores :

$$\begin{aligned} e_1 &= [\ 1,\ 0,\ 0,\ \ldots,\ 0\ ] \\ e_2 &= [\ 0,\ 1,\ 0,\ \ldots,\ 0\ ] \\ &\vdots \\ e_t &= [\ 0,\ 0,\ 0,\ \ldots,\ 1\ ] \end{aligned} \tag{IV-120}$$

É claro que esses vetores geram todos os elementos do anel Z_N , uma vez que cada elemento $x \in Z_N$ pode ser representado na forma :

$$\begin{aligned} x &= [\ x_1\ ,\ x_2\ ,\ldots,\ x_t\ ] = \\ &= [\ x_1,\ 0,\ldots,0\ ] + \ldots + [\ 0,\ldots,\ 0,\ x_t\ ] = \\ &= \sum_{i=1}^{t} e_i \,.\, x_i \end{aligned} \tag{IV-121}$$

onde $x_i \in Z_{N_i}$ ($i=1,\ldots,t$) .

Teorema IV-3 :

Para um dado anel Z_N ($N = N_1 \times \ldots \times N_t$ com $N_i = (p_i)^{\alpha_i}$, p_i primo para $i=1,\ldots,t$, $p_i \neq p_j$ para $i \neq j$ e sendo $\alpha_i = 1,2,\ldots$) , cada elemento $x \in Z_N$ pode ser representado na forma :

$$x = \sum_{i=t}^{t} x_i \cdot e_i \pmod{N} \qquad \text{(IV-122)}$$

sendo $x = [\, x_1,\ldots,x_t \,]$, $x_i \in Z_{N_i}$, e os vetores e_i (para $i=1,\ldots,t$) definidos em (IV-120) .

Em [42] são apresentadas as propriedades dos elementos idempotentes, como segue :

1ª - Cada elemento $x \in Z_N$ pode ser representado como um inteiro (forma radial) , ou como um vetor (forma modular) . Além disso, os vetores e_i ($i=1,\ldots,t$) geram um espaço linear que é isomórfico com o anel Z_N .

2ª - $$(e_i)^2 = e_i \pmod{N} \quad \text{para } i = 1,\ldots,t \qquad \text{(IV-123)}$$

3ª - $$\sum_{i=1}^{t} e_i = 1 \pmod{N} \qquad \text{(IV-124)}$$

4ª - $$\forall_{i \neq j} \; e_i \cdot e_j = 0 \pmod{N} \qquad \text{(IV-125)}$$

5ª - $$e_i \pmod{N_i} = 1 \quad \text{e} \quad \forall_{i \neq j} \; e_i \pmod{N_j} = 0 \qquad \text{(IV-126)}$$

IV.2.3.4.1 - CONCEITUAÇÃO BÁSICA

O sistema criptográfico de chave pública tipo mochila, que utiliza elementos idempotentes, proposto por PIEPRZYK e RUTKOWSKI [42], apresenta a formulação a seguir.

A geração da chave de cifrar em um criptossistema de chave pública é processada no lado do receptor.

Supondo que o receptor tenha escolhido inteiros N_1 , N_2 ,..., N_t , que são potências de diferentes números primos , ele pode determinar, para um dado valor secreto N , vetores (elementos idempotentes básicos) e_i , i=1,...,t , e obter a seqüência $a = (a_1,...,a_t)$ que gera todos os elementos do anel Z_N .

As mensagens a serem cifradas são da forma de uma seqüência $x = (x_1,...,x_t)$ onde x_i (i=1,...,t) é um inteiro, e $x \in Z_N$.

Tem-se então :

$$e = (e_1 , ..., e_t) \xrightarrow{\xi} a = (a_1 , ..., a_t)$$

onde ξ é uma transformação bijetora ("one-to-one") conhecida apenas pelo receptor.

Para a seqüência $a = (a_1,...,a_t)$ o receptor calcula o inteiro :

$$K = \max_{x} \left\{ \sum_{i=1}^{t} a_i \cdot x_i \right\} \qquad \text{(IV-127)}$$

e, então, escolhe, aleatoriamente, um par de inteiros (q, r) sendo $q > K$ e $r \neq 0$, $r \in Z_q$ (q é primo).

Os inteiros q e r podem ser usados para processar a transformação de cada elemento idempotente a_i , como segue :

$$m_i = a_i \cdot r \pmod{q} \quad , \quad i = 1,...,t \qquad \text{(IV-128)}$$

Assim é obtida a seqüência $\mathbf{m} = (m_1,\ldots,m_t)$, cujos elementos representam a chave pública de cifrar.

Neste sistema, o criptograma, para uma mensagem $x = (x_1,\ldots,x_t)$, é gerado de acordo com :

$$y = \sum_{i=1}^{t} m_i \cdot x_i \qquad \text{(IV-129)}$$

O criptograma é, então, transmitido ao receptor, onde o número y_r é calculado da forma :

$$y_r = y \cdot r^{-1} \pmod{q} \qquad \text{(IV-130)}$$

sendo r^{-1} o elemento inverso de r no anel Z_q .

Usando as equações (IV-128) e (IV-129) obtém-se :

$$y_r = \sum_{i=1}^{t} m_i . x_i . r^{-1} \pmod{q} = \sum_{i=1}^{t} a_i . x_i \pmod{q} \qquad \text{(IV-131)}$$

Como $q > K$, pode-se escrever :

$$y_r = \sum_{i=1}^{t} a_i \cdot x_i \qquad \text{(IV-132)}$$

O número y_r pode ser escrito, na forma modular, como um vetor projetado sobre os vetores a_i $(i=1,\ldots,t)$. Desta forma, para obter a mensagem $x = (x_1,\ldots,x_t)$ basta projetar o número y_r sobre os vetores $a_1,\ldots,a_t$, o que pode ser escrito como :

$$x_i = y_r \Big|_{a_i} \qquad \text{para} \quad i = 1,\ldots,t \qquad \text{(IV-133)}$$

Obtendo todos os componentes x_i da mensagem, o receptor pode, imediatamente, formar o texto claro.

A seguir serão apresentadas três formulações diferentes para o criptossistema de chave pública proposto.

1º CASO : ELEMENTOS IDEMPOTENTES BÁSICOS - SISTEMA BINÁRIO

Neste caso tem-se : $a = e$, isto é, $\xi = 1$.

Assim, seguindo a escolha da condição inicial para o criptossistema de chave pública (os inteiros $N_1,\ldots,N_t$), obtém-se os valores dos elementos idempotentes, que são convertidos em :

$$e_i \cdot r = m_i \pmod{q} \quad , \quad i=1,\ldots,t \qquad \text{(IV-134)}$$

onde o número primo q tem que satisfazer a inequação :

$$q > \max_{x} \left\{ \sum_{i=1}^{t} x_i \cdot e_i \right\} , \quad x = (x_1,\ldots, x_t) \qquad \text{(IV-135)}$$

e o inteiro r é aleatoriamente escolhido entre todos os elementos não-nulos do anel Z_q .

A chave pública $m = (m_1,\ldots,m_t)$ é enviada para o transmissor onde, para cada mensagem $x = (x_1,\ldots,x_t)$ o criptograma y é calculado conforme (IV-129).

O receptor do criptograma converte o valor recebido, obtendo :

$$y_r = y \cdot r^{-1} \pmod{q} \qquad \text{(IV-136)}$$

De posse do inteiro y_r , torna-se possível determinar a mensagem $x = (x_1,\ldots,x_t)$, cujos elementos são calculados como :

$$x_i = y_r \pmod{N_i} \quad , \quad i=1,\ldots,t \qquad \text{(IV-137)}$$

Da congruência (IV-137) conclui-se que, para obter a mensagem $x = (x_1,\ldots,x_t)$, a inequação :

$$x_i < N_i \quad , \quad i = 1,\ldots,t \qquad \text{(IV-138)}$$

deve ser obedecida. (Este valor máximo para x_i é tornado público; para mensagens binárias, $x_i \leq 1$).

Uma vez determinados todos os elementos x_i , encerra-se o processo de decifração.

A fim de diminuir a redundância característica de criptossistemas mochila, pode ser aplicada uma outra forma para obtenção do criptograma.

Assim, para uma chave pública $m = (m_1,\ldots,m_t)$ e uma mensagem $x = (x_1,\ldots,x_t)$, pode-se determinar o criptograma da seguinte forma :

$$y = \left| \sum_{j=1}^{u} x_{i_j} \cdot m_{i_j} - \sum_{j=u+1}^{t} x_{i_j} \cdot m_{i_j} \right| \qquad \text{(IV-139)}$$

onde a seqüência $x = (x_1,\ldots,x_t)$ é, aleatoriamente, dividida em duas subseqüências : $(x_{i_1},\ldots, x_{i_u})$ e $(x_{i_{u+1}},\ldots, x_{i_t})$

O processo de decifração, neste caso, é diferente, e, para decifrar o criptograma, algumas condições devem ser satisfeitas. Tais condições são apresentadas no teorema a seguir.

Teorema IV-4 :

A mensagem original pode ser reproduzida a partir do criptograma (IV-139) se, somente se, existir, pelo menos, um elemento $q_k \notin \{ -2, -1, 0, 1, 2 \} \subset Z_{N_k}$, onde $q_k = q \pmod{N_k}$, $1 \leq k \leq t$.

(Ver prova do teorema em [42])

O processo de decifração começa convertendo-se o criptograma y ,dado por (IV-139), em y_r , segundo (IV-136), obtendo-se :

$$y_r = y \cdot r^{-1} \pmod{q} = \qquad \text{(IV-140)}$$

$$= \left| \sum_{j=1}^{u} x_{i_j} \cdot e_{i_j} - \sum_{j=u+1}^{t} x_{i_j} \cdot e_{i_j} \right| \pmod{q}$$

onde : $e_{i_j} = m_{i_j} \cdot r^{-1}$, para $j=1,\ldots,t$.

A congruência (IV-140) tem duas soluções, a saber :

$$\cdot \quad y_r \pmod q \tag{IV-141}$$

$$\cdot \quad y'_r = -y_r = q - y_r \pmod q \tag{IV-142}$$

Para obter a mensagem a partir do criptograma, faz-se a projeção dos inteiros y_r e y'_r sobre os elementos idempotentes básicos, da seguinte forma :

$$y_r = [\, y_r \pmod{N_1}, \ldots, y_r \pmod{N_t} \,] = [\, y_{r_1}, \ldots, y_{r_t} \,]$$

$$y'_r = [\, y'_r \pmod{N_1}, \ldots, y'_r \pmod{N_t} \,] = [\, y'_{r_1}, \ldots, y'_{r_t} \,]$$

É claro que :

$$y_r + y'_r = q \quad , \tag{IV-143}$$

$$y_{r_i} + y'_{r_i} = q \pmod{N_i} \quad , \; i=1,\ldots,t$$

Como : $q \pmod{N_i} = q_i$, pode-se escrever :

$$y_{r_i} + y'_{r_i} = q_i \quad , \; i=1,\ldots,t \tag{IV-144}$$

Supondo que o inteiro y_r corresponde à mensagem **x** (o que significa que do inteiro y'_r não se pode extrair a mensagem), e que o criptossistema é usado para transmissão de mensagens binárias, vem :

$$y_{r_i} \in \{ -1, 0, 1 \} \subset Z_{N_i} \quad , \; i=1,\ldots,t \tag{IV-145}$$

Considerando (IV-144) e (IV-145), obtém-se :

$$y'_{r_i} \in \{ q_i - 1 \, , \, q_i \, , \, q_i + 1 \} \subset Z_{N_i} \tag{IV-146}$$

$$i=1,\ldots,t$$

Supondo ainda que exista, pelo menos, um elemento q_k satisfazendo :

$$\exists_{1 \leq k \leq t} \quad q_k \in \{ -2, -1, 0, 1, 2 \} \subset Z_{N_i} \quad , \qquad \text{(IV-147)}$$

e , usando a suposição de que o inteiro y_r corresponde à mensagem (isto é, $y_{r_i} \in \{ -1, 0, 1 \}$, i=1,...,t) , obtém-se :

$$y'_{r_i} \in \{ q_i - 1 \ , \ q_i \ , \ q_i + 1 \} \subset Z_{N_i}$$

Usando a expressão (IV-147) , vem :

$$\exists_{1 \leq k \leq t} \quad y'_{r_k} \in Z_{N_k} - \{ -1, 0, 1 \}$$

Assim, é possível, neste caso, distinguir o inteiro que não carrega a mensagem pois, para este inteiro, o seu k-ésimo elemento não pertence ao conjunto { -1, 0, 1 } .

Desta forma, se as condições do Teorema IV-4 forem satisfeitas então, no processo de decifração, deverão ser executados os seguintes procedimentos :

1º - Calcular os inteiros y_r e y'_r .

2º - Projetar esses inteiros sobre os elementos idempotentes básicos, obtendo duas seqüências.
(Lembrar que $q_i = y_{r_i} + y'_{r_i}$)

3º - De posse das duas seqüências obtidas, escolher aquela formada apenas por 0's(zeros) e 1's(uns), isto é: 0,-1,+1.

4º - A partir desta seqüência, detectar a mensagem como uma seqüência binária.

2º CASO : MATRIZ TRIANGULAR - SISTEMA BINÁRIO

Neste caso o vetor $e = (e_1,...,e_t)$ será considerado como definido em (IV-120), e os inteiros $N_1,...,N_t$ obedecendo as condições dadas por (IV-115).

O vetor e pode ser escrito sob a forma de matriz :

$$E = \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_t \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix} \qquad \text{(IV-148)}$$

Esta matriz pode ser convertida em uma matriz A usando-se alguma transformação como segue :

$$A = \begin{bmatrix} e_1+\dots+e_t \\ e_2+\dots+e_t \\ \vdots \\ e_{t-1}+e_t \\ e_t \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 0 & 1 & 1 & \dots & 1 & 1 \\ & & \vdots & & & \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{t-1} \\ a_t \end{bmatrix} \qquad \text{(IV-149)}$$

Conhecendo os valores dos elementos a_i , $i=1,..,t$, podem-se determinar os elementos da chave pública (lembrando que a escolha dos inteiros q e r é dada por (IV-127)), de acordo com a congruência :

$$m_i = a_i \cdot r \pmod{q} \quad , \quad i = 1,...,t \qquad \text{(IV-150)}$$

O criptograma será :

$$y = \sum_{i=1}^{t} x_i \cdot m_i \qquad \text{(IV-151)}$$

onde $x = (x_1,...,x_t)$ é a seqüência binária que representa a mensagem.

No lado do receptor, após receber o criptograma y, calcula-se o inteiro :

$$y_r = y \cdot r^{-1} \pmod{q} = \sum_{i=1}^{t} x_i \cdot a_i \pmod{q} \quad \text{(IV-152)}$$

e faz-se a projeção de y_r sobre os elementos idempotentes básicos $e_1,\ldots,e_t$, obtendo-se :

$$y_r = [\, y_{r_1}, \ldots, y_{r_t} \,] \quad \text{(IV-153)}$$

onde : $y_{r_i} = y_r \pmod{N_i}$, $i=1,\ldots,t$

Para obter-se o texto claro (mensagem), deve-se proceder da seguinte forma :

Passo 1 : Se $y_{r_1} = 0$, então $x_1 = 0$

Se $y_{r_1} = 1$, então $x_1 = 1$

Sejam definidos os inteiros d_i ($i = 2,\ldots,t$) da seguinte forma:

$$d_2 = y_r - x_1 \cdot a_1 \pmod{N} = [\, d_{21},\ldots,d_{2t} \,]$$

Passo 2 : Se $d_{22} = 0$, então $x_2 = 0$

Se $d_{22} = 1$, então $x_2 = 1$

Seja : $d_3 = d_2 - x_2 \cdot a_2 \pmod{N} = [\, d_{31},\ldots,d_{3t} \,]$

$\vdots$

Passo i : Se $d_{ii} = 0$, então $x_i = 0$

Se $d_{ii} = 1$, então $x_i = 1$

Seja : $d_{i+1} = d_i - x_i \cdot a_i \pmod{N} =$

$$= [\, d_{(i+1),1}, \ldots, d_{(i+1),t} \,] \ , \ i=3,\ldots,t$$

Assim recupera-se a mensagem $x = (x_1,\ldots,x_t)$.

Como no caso anterior, o criptograma pode também ser calculado conforme :

$$y = \left| \sum_{j=1}^{u} x_{i_j} \cdot m_{i_j} - \sum_{j=u+1}^{t} x_{i_j} \cdot m_{i_j} \right| \quad \text{(IV-154)}$$

sendo $m = (m_1, \ldots, m_t)$ definido em (IV-150) .

Neste caso, porém, algumas condições adicionais devem ser estabelecidas, em se tratando de criptossistema de chave pública, as quais estão definidas no teorema a seguir.

Teorema IV-5 :

A mensagem original pode ser recuperada a partir do criptograma (IV-154) se, somente se , o elemento q_1 satisfizer a condição $q_1 \notin \{ -2, -1, 0, 1, 2 \} \subset Z_{N_1}$, onde $q_1 = q \pmod{N_1}$, e o número primo q satisfaz a condição $q > \sum_{i=1}^{t} a_i$, para os inteiros a_i definidos em (IV-149).

(Ver prova do teorema em [42])

O processo de decifração começa convertendo-se o criptograma y , dado por (IV-154), no valor y_r ,definido em (IV-152), obtendo-se :

$$y_r = y \cdot r^{-1} \pmod{q}$$

$$= \left| \sum_{j=1}^{u} x_{i_j} \cdot a_{i_j} - \sum_{j=u+1}^{t} x_{i_j} \cdot a_{i_j} \right| \pmod{q} \quad \text{(IV-155)}$$

onde : $a_{i_j} = m_{i_j} \cdot r^{-1}$, para $j=1,\ldots,t$ conforme (IV-150).

Para determinar a mensagem, deve-se primeiro calcular dois inteiros diferentes que satisfaçam a congruência (IV-155):

. $y_r \pmod{q}$

. $y'_r = - y_r = q - y_r \pmod{q}$

Projetando-se esses inteiros sobre os elementos idempotentes básicos $e_1,\ldots,e_t$, obtém-se :

$$y_r = [\, y_r(\text{mod } N_1),\ldots,\, y_r(\text{mod } N_t)\,] = [\, y_{r_1},\ldots,\, y_{r_t}\,] \qquad \text{(IV-156)}$$

$$y'_r = [\, y'_r(\text{mod } N_1),\ldots,\, y'_r(\text{mod } N_t)\,] = [\, y'_{r_1},\ldots,\, y'_{r_t}\,] \qquad \text{(IV-157)}$$

Um dos elementos y_{r_1} ou y'_{r_1} , contendo o primeiro componente da mensagem, deve ser igual a um elemento pertencente ao conjunto $\{-1, 0, 1\} \subset Z_{N_1}$, pois a mensagem é uma seqüência binária .

Para determinar corretamente a mensagem, é necessário e suficiente que o primeiro elemento da seqüência que não carrega a mensagem, pertença ao conjunto $Z_{N_1} - \{-1, 0, 1\}$.

Se y_r contiver a mensagem, então :

$$y_{r_1} \in \{-1, 0, 1\}$$

e (IV-158)

$$y'_{r_1} \notin \{-1, 0, 1\}$$

Assim, como :

$$y_{r_1} + y'_{r_1} = q_1 \quad ,$$

onde : $q_1 = q \ (\text{mod } N_1)$,

tem-se que :

$$q_1 \notin \{-2, -1, 0, 1, 2\} \qquad \text{(IV-159)}$$

A escolha de q_1, de acordo com (IV-159), permite decidir, corretamente, qual a seqüência que carrega a mensagem já no primeiro passo do cálculo de y_r e y'_r.

A obtenção da mensagem (texto claro), a partir do criptograma y, segue o procedimento descrito abaixo :

1º - Calcular os inteiros y_r e y'_r.

2º - Projetar esses inteiros sobre os elementos idempotentes básicos, obtendo duas seqüências.
(Lembrar que $q_i = y_{r_i} + y'_{r_i}$)

3º - Selecionar a seqüência cujo primeiro elemento pertence ao conjunto $\{ -1, 0, 1 \}$.

4º - De posse dessa seqüência, aplicar o algoritmo para obtenção da seqüência $x = (x_1, \ldots, x_t)$, que representa a mensagem, conforme descrito acima.

3º CASO : MATRIZ "DIAGONAL DUPLA" - SISTEMA BINÁRIO

Neste caso será considerada uma maneira diferente para formação da matriz A .

Supondo que a matriz E seja definida como mostrado em (IV-148) , a matriz A será :

$$A = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{t-1} \\ a_t \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 & 0 \\ & & \vdots & & & & \\ 0 & 0 & 0 & 0 & \dots & 1 & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix} = \begin{bmatrix} e_1 + e_2 \\ e_2 + e_3 \\ \vdots \\ e_{t-1} + e_t \\ e_t + e_1 \end{bmatrix} \qquad \text{(IV-160)}$$

Seja a chave pública obtida da mesma forma como anteriormente descrita em (IV-150), onde :

$$m_i = a_i \cdot r \pmod q \quad , \quad i=1,\dots,t \quad ,$$

porém, com o número primo q satisfazendo a desigualdade :

$$q > \left\{ \sum_{i=1}^{t-1} a_i \cdot a_{i+1} \right\} + a_1 \cdot a_t \qquad \text{(IV-161)}$$

e o inteiro r escolhido, aleatoriamente, dentre os elementos do anel Z_q , sendo $r \neq 0$.

O criptograma correspondente a um bloco de mensagem binária de t bits, $x = (x_1,\dots,x_t)$, é produzido como :

$$y = \left| \sum_{j=1}^{u} x_{i_j} \cdot w_{i_j} - \sum_{j=u+1}^{t} x_{i_j} \cdot w_{i_j} \right| \qquad \text{(IV-162)}$$

onde : $w_1 = m_1 \cdot m_t$,

$w_i = m_{i-1} \cdot m_i$ para $i=2,\ldots,t$, e

$w_{i_j} \in \{ w_1 , \ldots , w_t \}$.

No lado do receptor, pode-se calcular y_r , a partir do valor do criptograma y recebido, fazendo :

$$y_r = y \cdot r^{-2} \pmod{q} \qquad \text{(IV-163)}$$

Considerando as congruências :

$$w_1 = m_1 \cdot m_t = r^2 \cdot a_1 \cdot a_t = r^2 \cdot e_1 \pmod{q}$$

e

$$w_i = m_{i-1} \cdot m_i = r^2 \cdot a_{i-1} \cdot a_i = r^2 \cdot e_i \pmod{q} , \quad i=2,\ldots,t$$

então a expressão (IV-163) pode ser escrita como :

$$y_r = \left| \sum_{j=1}^{u} x_{i_j} . e_{i_j} - \sum_{j=u+1}^{t} x_{i_j} . e_{i_j} \right| \pmod{q} \qquad \text{(IV-164)}$$

Da mesma forma mostrada anteriormente, podem-se calcular y_r e y'_r , onde $y_r + y'_r = q$.

Assim, tendo calculado o par de valores y_r e y'_r , procede-se como no 1º CASO (descrito anteriormente), para recuperar a mensagem a partir do criptograma y recebido.

IV.2.3.4.2 - EXEMPLOS DE APLICAÇÃO

Para ilustrar o método criptográfico apresentado em [42] , seguem-se os exemplos numéricos :

1º - Elementos Idempotentes Básicos sem transformação

Seja o sistema criptográfico para cifrar mensagens binárias de 4 bits (t=4) .

Sejam considerados os primos :

$$N_1=2 \quad , \quad N_2=3 \quad , \quad N_3=5 \quad , \quad N_4=7$$

que fornecem :

$$N = 2 \times 3 \times 5 \times 7 \qquad \therefore \qquad N = 210$$

Para estes valores, e aplicando o Teorema Chinês do Resto, os elementos idempotentes básicos podem ser representados como :

$$\begin{aligned} e_1 &= [\ 1,\ 0,\ 0,\ 0\ ] = 105 \\ e_2 &= [\ 0,\ 1,\ 0,\ 0\ ] = 70 \\ e_3 &= [\ 0,\ 0,\ 1,\ 0\ ] = 126 \\ e_4 &= [\ 0,\ 0,\ 0,\ 1\ ] = 120 \end{aligned}$$

Assim sendo :

$$a = e = (\ 105,\ 70,\ 126,\ 120\ )$$

Escolhendo um primo $q = 431$ ($> 105+70+126+120$) , e um inteiro $r = 108$ $\therefore$ $r^{-1} = 4 \bmod 431$, a chave pública pode ser calculada conforme (IV-134) , obtendo-se :

$$m = (\ m_1, m_2, m_3, m_4\ ) = (\ 134,\ 233,\ 247,\ 30\ )$$

Considerando a mensagem $x = (\ 1,\ 0,\ 1,\ 1\ )$, o criptograma a ser enviado ao receptor será :

$$y = 134 + 247 + 30 \qquad \therefore \qquad y = 411$$

O receptor, para recuperar a mensagem, calcula :

$$y_r = y \cdot r^{-1} \pmod{q}$$

$$y_r = 411 \times 4 \pmod{431} \quad \therefore \quad y_r = 351$$

e efetua :

$$x_i = y_r \pmod{N_i} \qquad i=1,2,3,4$$

$$x_1 = 351 \bmod 2 = 1$$
$$x_2 = 351 \bmod 3 = 0$$
$$x_3 = 351 \bmod 5 = 1$$
$$x_4 = 351 \bmod 7 = 1 \quad ,$$

recuperando a mensagem : $x = (x_1, x_2, x_3, x_4) = (1, 0, 1, 1)$

Com a finalidade de diminuir a redundância gerada no processo de cifração, o criptograma poderia ter sido calculado como :

$$y = -134 + 247 - 30 \quad \therefore \quad y = 83$$

Neste caso, o receptor deverá executar as seguintes operações para recuperar a mensagem :

- Calcular dois elementos : y_r e y'_r

$$y_r = y \cdot r^{-1} \pmod{q} = 83 \times 4 \bmod 431 = 332$$
$$y'_r = q - y_r = 431 - 332 = 99$$

- Determinar os componentes de y_r e y'_r da representação modular :

$$y_r = 332 \leftrightarrow [0, 2, 2, 3]$$
$$y'_r = 99 \leftrightarrow [1, 0, 4, 1] = [1, 0, -1, 1]$$

A partir dessas duas seqüências, o receptor pode, facilmente, determinar a mensagem (a partir de y'_r) :

$$x = (x_1, x_2, x_3, x_4) = (1, 0, 1, 1)$$

2º - Caso da Matriz Triangular Superior

Seja o sistema criptográfico para cifrar mensagens binárias de 4 bits (t=4).

Sejam considerados os primos :

$$N_1=2 \quad , \quad N_2=3 \quad , \quad N_3=5 \quad , \quad N_4=7 \quad ,$$

que fornecem :

$$N = 2 \times 3 \times 5 \times 7 \quad \therefore \quad N = 210$$

Para estes valores, as matrizes E e A , definidas em (IV-148) e (IV-149), respectivamente, assumem os seguintes valores :

$$E = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 105 \\ 70 \\ 126 \\ 120 \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 316 \\ 246 \\ 120 \end{bmatrix}$$

Assim sendo, tem-se :

$$a = (a_1, a_2, a_3, a_4) = (1, 316, 246, 120)$$

Escolhendo um primo $q = 719$ (> 1+316+246+120) , e um inteiro $r = 299 \quad \therefore \quad r^{-1} = 101 \bmod 719$, a chave pública de cifrar pode ser calculada conforme (IV-150), obtendo-se :

$$m = (m_1, m_2, m_3, m_4) = (299, 295, 216, 649)$$

Considerando a mensagem binária $x = (1, 0, 1, 1)$, o criptograma correspondente, a ser enviado ao receptor, será:

$$y = 299 + 216 + 649 \quad \therefore \quad y = 1164$$

O receptor, de posse do criptograma, calcula :

$$y_r = y \cdot r^{-1} \pmod{q}$$

$$y_r = 1164 \times 101 \pmod{719} \quad \therefore \quad y_r = 367$$

e efetua :

$$y_{ri} = y_r \pmod{N_i} \qquad i=1,2,3,4$$

$$y_{r_1} = 367 \mod 2 = 1$$
$$y_{r_2} = 367 \mod 3 = 1$$
$$y_{r_3} = 367 \mod 5 = 2$$
$$y_{r_4} = 367 \mod 7 = 3 \quad .$$

Usando o algorimo de decifração vem :

$i=1$, $y_{r_1} = 1$, então $x_1 = 1$

$$d_2 = y_r - x_1 a_1 \pmod{N} = 367 - 1$$
$$d_2 = 366 = [0, 0, 1, 2]$$

$i=2$, $d_{22} = 0$, então $x_2 = 0$

$$d_3 = d_2 - x_2 a_2 \pmod{N} = 366 - 0$$
$$d_3 = 366 = [0, 0, 1, 2]$$

$i=3$, $d_{33} = 1$, então $x_3 = 1$

$$d_4 = d_3 - x_3 a_3 \pmod{N} = 366 - 246 \bmod 210$$
$$d_4 = 330 = [0, 0, 0, 1]$$

$i=4$, $d_{44} = 1$, então $x_4 = 1$

Desta forma : $x = (x_1, x_2, x_3, x_4) = (1, 0, 1, 1)$

IV.2.3.4.3 - COMENTÁRIOS

O criptossistema utilizando elementos idempotentes proposto por PIEPRZYK e RUTKOWSKI [42] pode ser considerado como uma modificação do sistema de MERKLE e HELLMAN [3]. Sua formulação muito se assemelha ao esquema apresentado por GOODMAN e McAULEY [44] : a idéia básica da formulação é muito boa e, segundo certos aspectos, pode ser considerada como um esquema mais geral que este último.

Neste sistema, a chave de cifrar é gerada a partir de uma seqüência formada pela representação radial de vetores adequados (usando números primos e o Teorema Chinês do Resto), à qual é aplicada uma transformação modular.

A implementação de elementos idempotentes num sistema criptográfico não apenas permite um enfoque mais elástico quanto ao problema de ajuste do algoritmo de cifração à forma da mensagem, mas também possibilita a decifração simples dos criptogramas gerados.

O criptossistema utilizando elementos idempotentes apresenta as seguintes vantagens :

- capacidade de fácil adaptação do criptossistema para transmissão de mensagens não-binárias (mas o algoritmo apresenta melhor desempenho para mensagens binárias) ;

- exigência de solução, por parte de um receptor não autorizado , de um problema mochila mais complicado (porque os criptogramas são calculados conforme a equação (IV-139), em vez da (IV-129)) ;

- diminuição da redundância dos criptogramas, devido a uma escolha apropriada das somas definidas em (IV-139).
  (Esta pode ser considerada a maior vantagem do método).

Uma desvantagem apresentada por este criptossistema é o tamanho da chave pública, que é da ordem de alguns milhares de bits.

O usuário deste sistema criptográfico deve ficar atento à escolha dos parâmetros utilizados no processo de obtenção da chave pública, para evitar que seja gerada uma mochila de fácil solução (como, por exemplo, seqüência supercrescente ou com elemento dominante).

Do ponto de vista da segurança criptográfica do sistema apresentado em [42], pode-se afirmar que o mesmo resiste aos ataques de recuperação da informação "trapdoor" [25], [27] e [29], pois não utiliza seqüências supercrescentes.

No entanto, nada se pode garantir quanto à resistência do sistema aos ataques por reduções sucessivas [6], [21] e [26] , nem aos ataques a mochilas de baixa densidade [35] e [43].

O fato deste criptossistema empregar um modo mais complicado para obtenção dos criptogramas, e também de utilizar a multiplicação de números primos como um dos parâmetros secretos que gerarão a chave pública, dificulta o trabalho de criptoanálise da mensagem por um interceptador, caracterizando, assim, um sistema mais seguro, quando comparado ao SCMH.

IV.2.4 - SISTEMA MOCHILA EM CORPOS FINITOS

IV.2.4.1 - UTILIZAÇÃO DE POLINÔMIOS

Apesar de alguns ataques criptoanalíiticos apresentados no Capítulo III mostrarem que o SCMH não é seguro (sob certas condições) para ser utilizado como um algoritmo de cifração de chave pública, continua o interesse nos criptossistemas mochila devido à sua inerente simplicidade. Por esta razão, em 1984, COOPER e PATTERSON [41] sugeriram uma generalização para o sistema criptográfico de chave pública , usando o conceito de polinômios irredutíveis em Corpo de Galois, a fim de gerar um criptossistema mais seguro às investidas criptoanalíticas.

O algoritmo original de MERKLE-HELLMAN [3] utiliza a propriedade de que os inteiros,módulo um número primo, formam um corpo finito; existe, porém, uma classe mais rica de corpos finitos.(Na realidade, para Merkle-Hellman, basta que os inteiros tenham a estrutura de anel, e não de corpo.)

O anel dos quocientes dos polinômios com coeficientes em Z_p , módulo um polinômio irredutível em Z_p de grau n, é um corpo finito de p^n elementos. Esses corpos são chamados Corpos de Galois.

A notação para congruência em um corpo de p^n elementos é definida como :

$$r(x) \equiv s(x) \mod (p, I(x)) \qquad \text{(IV-165)}$$

onde: p é o número primo indicando o corpo dos coeficientes ;
I(x) é um polinômio irredutível sobre Z_p .

A seguir são apresentadas as formulações de COOPER e PATTERSON [41] e de PAZ DE LIMA [52] , que utilizam polinômios.

IV.2.4.1.1 - CONCEITUAÇÃO BÁSICA

IV.2.4.1.1.1 - FORMULAÇÃO DE COOPER E PATTERSON

Do mesmo modo que o método original de Merkle-Hellman passa de um anel Z de inteiros para um anel associado Z_m, assim também a generalização proposta por COOPER e PATTERSON [41] começará com um conjunto mochila em $Z[x]$, e passará para um Corpo de Galois associado. A generalização do processo de geração da chave pública é caracterizada pelo algoritmo a seguir :

1º PASSO : Escolher, segundo um dos dois métodos apresentados adiante, um conjunto mochila "fácil" de n polinômios $a'_i(x)$ no anel dos polinômios sobre os inteiros. Escolher todos os polinômios de mesmo grau k.

2º PASSO : Determinar um número primo m, maior que duas vezes o maior coeficiente de todos os polinômios.

3º PASSO : Determinar um polinômio irredutível sobre Z_m, $I(x)$, de grau igual a $k+1$.

4º PASSO : Escolher um outro polinômio sobre Z_m, $w(x)$, de grau menor ou igual a k.

5º PASSO : Gerar um conjunto mochila "difícil" de polinômios $a_i(x)$, usando a transformação :

$$a_i(x) \equiv a'_i(x) \cdot w(x) \bmod (m, I(x)) \qquad \text{(IV-166)}$$

(Não se pode garantir que os polinômios $a_i(x)$ sejam "difíceis".)

Este sistema reflete, exatamente, a transformação utilizada no esquema de Merkle-Hellman; de fato, para $k=0$ recai-se neste caso.

Para o criptossistema apresentado em [41], as operações de cifração e de decifração se processam de maneira similar às do SCMH .

O trasmissor da mensagem cifra uma seqüência de n bits, $b = (b_1,\ldots,b_n)$, multiplicando cada bit por um polinômio $a_i(x)$ e transmite os coeficientes do polinômio $S(x)$ resultante :

$$S(x) = b_1 \cdot a_1(x) +\ldots+ b_n \cdot a_n(x) \qquad \text{(IV-167)}$$

Para decifrar a mensagem, o receptor multiplica $S(x)$ pelo polinômio que é o inverso de $w(x)$ mod $(m, I(x))$, denominado de $w^{-1}(x)$, obtendo :

$$S'(x) = S(x) \cdot w^{-1}(x) \bmod (m, I(x)) \qquad \text{(IV-168)}$$

$$S'(x) = b_1 \cdot a'_1(x) +\ldots+ b_n \cdot a'_n(x) \quad , \qquad \text{(IV-169)}$$

e assim pode, facilmente, recuperar a mensagem em texto claro $b = (b_1,\ldots,b_n)$, pois os polinômios $a'_i(x)$ formam uma mochila "fácil".

Segundo COOPER e PATTERSON [41], dois métodos podem ser utilizados para selecionar um conjunto mochila "fácil" no anel dos polinômios sobre os inteiros, para iniciar o processo de geração da chave pública.

1º MÉTODO : Este método é uma versão vetorial simples do método proposto por Merkle-Hellman. Isto é, se o polinômio $a'_i(x)$ for escrito como :

$$a'_i(x) = a'_{i,k} \cdot x^k + a'_{i,k-1} \cdot x^{k-1} +\ldots+ a'_{i,1} \cdot x + a'_{i,0} \qquad \text{(IV-170)}$$

$$i=1,\ldots,n$$

então cada conjunto $\{ a'_{1,j}, a'_{2,j},\ldots, a'_{n,j} \}$ de coeficientes do termo de grau j será escolhido para formar uma seqüência supercrescente.

Uma das críticas ao esquema de Merkle-Hellman tem sido o tamanho das chaves necessárias para a transmissão das mensagens. O segundo método para escolha dos coeficientes melhora este problema.

2º MÉTODO : Um método alternativo para escolher um conjunto mochila fácil executa o seguinte procedimento:

1 - Decidir quantos bits deverá conter a seqüência que representa a mensagem original a ser cifrada com apenas uma aplicação do algoritmo. Denominar este número de N .

2 - Particionar N em um conjunto de s inteiros, definido como $R = \{ r_1, r_2, \ldots, r_s \}$, tal que :

$$r_1 + r_2 + \ldots + r_s = N \qquad \text{(IV-171)}$$

3 - Para cada i=1,2,...,s , gerar seqüências de r_i números "mochila-fácil" , como no método anterior. Os conjuntos devem ser escolhidos independentemente um do outro.

4 - Gerar uma matriz nula A de dimensão (N x s) e colocar um dos s conjuntos de números "mochila-fácil" em cada coluna desta matriz. Os r_i números em cada conjunto podem ser colocados em qualquer das linhas de sua respectiva coluna, mas cada linha da matriz A deverá conter um número "mochila-fácil" em uma , e somente uma, de suas colunas ao final do processo.
Este número "mochila-fácil" é dito "cobrir" a linha em que se encontra. Como existe um total de N números "mochila-fácil", cada linha é coberta exatamente uma vez. Os coeficientes $A_{i,j}$ da matriz A são, agora, usados para construir os polinômios $a'_i(x)$.

A vantagem do segundo método de escolha de polinômios fáceis recai no tamanho das chaves associadas.

A geração da chave pública de cifrar se processa como descrito no algoritmo apresentado anteriormente.

IV.2.4.1.1.2 - FORMULAÇÃO DE PAZ DE LIMA

Em 1983 PAZ DE LIMA [52] apresentou, sem, no entanto, publicar, uma formulação para o criptossistema mochila utilizando como chave secreta de decifrar uma seqüência cujos elementos são potências de um número inteiro adequado, e uma matriz, como multiplicador desta seqüência, para gerar a chave pública de cifrar. (Não é utilizada a tradicional transformação modular) . Esta formulação pode ser considerada como um caso particular do método de polinômios proposto por COOPER e PATTERSON [41].

Na formulação apresentada em [52], seja a seqüência $a' = (a'_1,...,a'_r)$ supercrescente e seja uma matriz A qualquer de dimensão (n x r) (esta matriz não precisa ter inversa), tal que :

$$a'_i = b^{i-1} \quad , \quad i=1,2,...,r \qquad \text{(IV-172)}$$

$$b > \max_i \left\{ \sum_{j=1}^{n} A_{ji} \right\}, \quad i=1,2,...,r \qquad \text{(IV-173)}$$

isto é, a base b da potência formadora dos elementos da seqüência supercrescente tem que ser maior que a maior soma dos elementos das colunas da matriz A .

A matriz A , de dimensão (n x r) é escolhida de forma que suas colunas sejam seqüências difíceis, mas existe uma combinação linear dessas colunas que gera uma seqüência fácil.

O vetor $a' = (a'_1,...,a'_r)$, a matriz A , e a combinação linear (definida pelos inteiros k_i , i=1,...,r) são mantidos secretos.

O fato de se utilizar uma matriz não quadrada serve , também, para esconder a dimensão do vetor secreto supercrescente.

O vetor $a = (a_1,...,a_n)$ pode ser obtido pelo produto matricial definido por :

$$(a)^T = A . (a')^T$$

ou

$$a = a' . A^T \qquad \text{(IV-174)}$$

onde : A é a matriz secreta : n x r

$a' = (a'_1,...,a'_r)$ é a chave secreta supercrescente

$a = (a_1,...,a_n)$ é a chave pública de cifrar.

Para cifrar um vetor-mensagem $x = (x_1,...,x_n)$, de dimensão n , o usuário deve calcular o criptograma S da seguinte forma :

$$S = a . x^T \qquad \text{(IV-175)}$$

que pode ser escrito, usando (IV-174), como :

$$S = (a' . A^T) . x^T \quad ,$$

ou ainda,

$$S = a'_1 . (A^{(1)} . x) + a'_2 . (A^{(2)} . x) +...+ a'_r . (A^{(r)} . x)$$

$$S = \sum_{i=1}^{r} a'_i . (A^{(i)} . x) \qquad \text{(IV-176)}$$

onde : $A^{(i)}$ é a i-ésima coluna da matriz A : 1 x n

a'_i é o i-ésimo elemento do vetor a' : 1 x r

$x = (x_1,...,x_n)$ é o vetor-mensagem : 1 x n

Pela expressão (IV-176) observa-se que o criptograma obtido é uma "combinação linear de mochilas" e , portanto, é uma generalização do SCMH, onde o multiplicador escalar foi substituído por uma matriz.

Uma vez recebido o criptograma S , o receptor autorizado pode recuperar a mensagem $x = (x_1,\ldots,x_n)$, efetuando o seguinte procedimento :

1º - Determinar os inteiros :

$$B_i = A^{(i)} . x \quad , \quad i=1,\ldots,r$$

conhecido o criptograma S , pois :

$$S = \sum_{i=1}^{r} a'_i . (A^{(i)} . x) = \sum_{i=1}^{r} a'_i . B_i \qquad \text{(IV-177)}$$

A seqüência $B = (B_1,\ldots,B_r)$ pode ser facilmente determinada empregando-se o Teorema Fundamental da Divisão, uma vez que os elementos do vetor $a' = (a'_1,\ldots,a'_r)$ são potências de base constante. Os elementos B_i , $i=1,\ldots,r$ são chamados de coeficientes da representação do criptograma S na base b .

2º - Usar a combinação linear secreta, caracterizada pelos coeficientes inteiros k_i , $i=1,\ldots,r$ (que podem ser positivos, negativos ou nulos) , que gera a seqüência de fácil solução, para obter o vetor-mensagem $x = (x_1,\ldots, x_n)$:

$$k_1.B_1 + k_2.B_2 + \ldots + k_r.B_r = \ldots \qquad \text{(IV-178)}$$

$$\ldots = (k_1.A^{(1)} + k_2.A^{(2)} + \ldots + k_r.A^{(r)}) . x^T$$

Como a seqüência que multiplica o vetor-mensagem x é fácil (pode até ser supercrescente), e também são conhecidos todos os termos do lado direito da equação (IV-178), a recuperação da mensagem $x = (x_1,\ldots,x_n)$ torna-se trivial.

A essência dessa formulação é utilizar combinações lineares de seqüências difíceis (colunas da matriz A) para obter uma seqüência de fácil solução, utilizando um vetor especial supercrescente. Neste sistema ocorre a substituição do multiplicador escalar do SCMH pela matriz A, usada para gerar a chave pública de cifrar. Uma desvantagem dessa formulação é a grande expansão de dados gerada no processo de cifração.

IV.2.4.1.2 - EXEMPLO DE APLICAÇÃO

O exemplo numérico apresentado a seguir ilustra a formulação do criptossistema de PAZ DE LIMA [52].

Seja definida a seguinte matriz A , de dimensão 4 x 4:

$$A = \begin{bmatrix} 2 & 12 & 5 & 1 \\ 4 & 9 & 3 & 7 \\ 6 & 10 & 2 & 2 \\ 8 & 1 & 2 & 9 \end{bmatrix}$$

Sejam escolhidos : $k_1=7$, $k_2=-1$, $k_3=k_4=0$.

Assim, a combinação linear das colunas da matriz A fornecerá a seguinte seqüência supercrescente :

$$7 \cdot A^{(1)} - A^{(2)} = [\ 14, 28, 42, 56\ ] - [\ 12, 9, 10, 1\ ]$$
$$= [\ 2, 19, 32, 55\ ] \quad ,$$

onde $A^{(i)}$ é a i-ésima coluna da matriz A .

Escolhendo b = 43 satisfazendo (IV-173), isto é, maior que a soma dos elementos de cada coluna da matriz, pode-se construir o vetor $a' = (a'_1, a'_2, a'_3, a'_4)$ da seguinte forma :

$$a'_i = b^{i-1} \quad , \quad i=1,2,3,4$$

$$a'_1 = 43^0 = 1$$
$$a'_2 = 43^1 = 43$$
$$a'_3 = 43^2 = 1849$$
$$a'_4 = 43^3 = 79507$$

$$a' = (1, 43, 1849, 79507)$$

A chave pública de cifrar $a = (a_1, a_2, a_3, a_4)$ é obtida efetuando-se :

$$(a)^T = A \cdot (a')^T \quad ,$$

que, para os valores acima, fornece :

$$a = (89270, 562487, 163148, 719312)$$

Para o vetor-mensagem $x = (0, 1, 1, 0)$, o criptograma correspondente será :

$$S = a \cdot x^T \qquad \therefore \qquad S = 725635$$

Para decifrar o criptograma recebido e recuperar a mensagem, o receptor calcula :

$$S = a'_1 B_1 + a'_2 B_2 + a'_3 B_3 + a'_4 B_4$$

$$725635 = B_1 + 43.B_2 + 1849.B_3 + 79507.B_4$$

(Observe-se a semelhança com o método de polinômios apresentado em [41]).

Empregando-se o Teorema Fundamental da Divisão, obtêm-se os elementos B_i , $i=1,2,3,4$:

$$725635 = 79507.B_4 + r_4 \quad \rightarrow \quad B_4 = 9, \; r_4 = 10072$$

$$10072 = 1849.B_3 + r_3 \quad \rightarrow \quad B_3 = 5, \; r_3 = 827$$

$$827 = 43.B_2 + r_2 \quad \rightarrow \quad B_2 = 19, \; r_2 = 10$$

$$10 = 1.B_1 + r_1 \quad \rightarrow \quad B_1 = 10, \; r_1 = 0$$

Como o receptor autorizado conhece a matriz secreta A e a combinação linear das colunas que gera a seqüência supercrescente, ele pode, então, calcular :

$$7 . B_1 - B_2 = (7 . A^{(1)} - A^{(2)}) . x^T$$

$$51 = [2, 19, 32, 55] . x^T$$

A obtenção do vetor $x = (x_1, x_2, x_3, x_4)$ é trivial, porque a seqüência que o multiplica é supercrescente. Assim :

$$x = (x_1, x_2, x_3, x_4) = (0, 1, 1, 0)$$

IV.2.4.1.3 - COMENTÁRIOS

O sistema criptográfico de chave pública, proposto por COOPER e PATTERSON [41], baseado no conceito de Corpos Finitos é uma extensão natural do SCMH para cifração de dados.

Como desvantagens deste sistema podem ser citadas a expansão de dados gerada no processo de cifração, e o fato de consumir muita memória para armazenar as chaves de cifrar de todos os usuários, que agora são um conjunto de polinômios e não mais seqüência de inteiros.

No primeiro passo do algoritmo de geração da chave de cifrar foi imposta a condição de todos os polinômios escolhidos para formar a chave secreta, terem o mesmo grau. Na realidade os polinômios não precisam ter o mesmo grau para o sistema funcionar, e é até melhor que não tenham.

No caso do primeiro método de escolha do conjunto "mochila-fácil" foi dito que os coeficientes de todos os termos de cada grau devem formar uma seqüência supercrescente. No entanto, basta que os coeficientes dos termos de um certo grau formem uma seqüência supercrescente, permitindo a identificação dos polinômios que foram considerados no cálculo do criptograma. Desta forma, as colunas da matriz de coeficientes (cada coluna correspondente a um grau do polinômio) não precisam ser todas elas mochilas fáceis (supercrescentes por grau), para não fornecer muita informação ao adversário.

Pode-se utilizar, segundo PAZ DE LIMA [52], matriz cujas colunas são aleatórias (difíceis), mas tal que exista uma combinação linear delas que gere uma seqüência supercrescente. Assim, são eliminadas duas desvantagens : não é dada informação adicional ao inimigo, pois não teria duas ou mais colunas diferentes com a mesma solução ; a matriz não precisa ser cheia, podendo ter elementos nulos.

Quanto à segurança criptográfica dos sistemas apresentados em [41] e [52], pode-se afirmar que estes resistem aos ataques de recuperação da informação "trapdoor" [25], [27] e [29], devido às características de sua construção.

Nada se pode garantir, no entanto, quanto à resistência destes sistemas aos ataques por reduções sucessivas [6], [21] e [26], e nem aos ataques a mochilas de baixa densidade [35] e [43].

IV.2.4.2 - UTILIZAÇÃO DE LOGARITMO DISCRETO

Criptossistemas mochila de chave pública são baseados na intratabilidade de encontrar uma solução para $S = \Sigma\, x_i a_i$, mesmo quando se sabe que existe uma solução.

Em tais sistemas, cada usuário publica uma seqüência A de elementos a_i e um limite $h \geq \Sigma\, x_i$.

Uma mensagem em texto claro consistindo de um vetor inteiro $X = (x_0, x_1, \ldots, x_{n-1})$, com peso menor ou igual a h (onde peso de um vetor é o número de elementos não-nulos neste vetor), é cifrada da seguinte forma :

$$E(X) = \sum_{i=0}^{n-1} x_i \cdot a_i \qquad \text{(IV-179)}$$

Os elementos a_i do vetor mochila são escolhidos de forma que a equação (IV-179) seja facilmente resolvida se certa informação "trapdoor" secreta for conhecida. A natureza exata desta informação depende do sistema particular em questão.

Uma propriedade geral dos criptossistemas de chave pública tipo mochila é que a cifração é fácil, tudo que se precisa fazer é somar (no caso de sistemas binários), ou multiplicar e somar (no caso de sistemas não-binários).

Em 1984 CHOR e RIVEST [55] propuseram um novo criptossistema mochila de chave pública que possui alta densidade e cujos conceitos básicos diferem, um pouco, daqueles utilizados nos demais criptossistemas desse tipo. Este sistema utiliza um resultado devido a Bose e Chowla, sobre representação única de somas em seqüências finitas "densas". Para criar chaves de cifrar e de decifrar nesta construção, são calculados logaritmos discretos em Corpos Finitos. A cifração se processa muito rapidamente (tempo linear), e a decifração é razoavelmente rápida (comparada com o RSA), sendo a criação das chaves a parte mais difícil. Para uma escolha adequada do Corpo Finito a ser utilizado, os autores acreditam que o sistema obtido con

seguirá frustrar os ataques de baixa densidade e de busca exaustiva.

Dados n e h, inteiros não-negativos, existe uma seqüência $A = \{ a_i \mid 0 \leq i \leq n-1 \}$ de inteiros não-negativos, tal que todas as somas de exatamente h elementos (repetições permitidas) de A sejam distintas ?

É fácil construir tais seqüências se os elementos a_i forem crescentes exponencialmente em n : por exemplo a seqüência $\{ 1, h, h^2, \ldots, h^{n-1} \}$ tem a propriedade acima. Mas é possível construir tal seqüência com os elementos a_i crescendo apenas polinomialmente em n ?

Bose e Chowla determinaram uma forma muito elegante de construir tais seqüências com $1 \leq a_i \leq n^h - 1$, $i=0,\ldots,n-1$.

Teorema IV-6 : Teorema Bose-Chowla

Seja p um número primo, $h \geq 2$ um inteiro. Então existe uma seqüência $A = \{ a_i \mid 0 \leq i \leq p-1 \}$ de inteiros tal que :

(1) $1 \leq a_i \leq p^h - 1$, $i = 0,1,\ldots,p-1$

(2) Se $(x_0, x_1, \ldots, x_{p-1})$ e $(y_0, y_1, \ldots, y_{p-1})$ forem dois vetores distintos, com coordenadas inteiras não-negativas, e :

$$\sum_{i=0}^{p-1} x_i \leq h \quad , \quad \sum_{i=0}^{p-1} y_i \leq h$$

então tem-se que :

$$\sum_{i=0}^{p-1} x_i \cdot a_i \neq \sum_{i=0}^{p-1} y_i \cdot a_i$$

Vale ressaltar que a condição " p é um número primo " pode ser substituída por " p é uma potência de primo " , sem alterar o teorema e sua prova. Também, pela prova do teorema mostrada em [55], fica claro que ℓ somas ($\ell \leq h$) de elementos de A são distintas, não apenas sobre $\mathbb{Z}$, mas também considerando módulo $p^h - 1$.

IV.2.4.2.1 - CONCEITUAÇÃO BÁSICA

A formulação do sistema criptográfico proposto por CHOR e RIVEST [55] é apresentada a seguir, onde são descritos o processo de geração da chave de cifrar, e os procedimentos de cifração e de decifração.

- GERAÇÃO DO SISTEMA

Para obtenção da chave pública de cifrar, o usuário deve executar os seguintes passos :

1º - Escolher p , uma potência de primo, e $h \leq p$, um inteiro positivo , tais que logaritmos discretos no Corpo Finito $GF(p^h)$ possam ser calculados de maneira eficaz.

(Conforme mostrado por POHLIG e HELLMAN [31], determinar logaritmos sobre $GF(p^h)$ é relativamente fácil se $p^h - 1$ tiver somente fatores primos pequenos. Em um computador, o valor corrente para o limite superior de "pequeno" é da ordem de 10^6 a 10^{12}.)

2º - Escolher um aleatório $t \neq 0 \in GF(p^h)$ algébrico de grau h em $GF(p)$. Isso será feito determinando-se $f(t)$, um polinômio mônico aleatório irredutível de grau h em $GF(p)[t]$, e representando-se a aritmética $GF(p^h)$ por $GF(p)[t]/ < f(t) >$. (Isto é, os elementos de $GF(p^h)$ são polinômios de grau menor ou igual a $h-1$ com coeficientes em $GF(p)$, e as operações de adição/multiplicação são feitas módulo p e $f(t)$.)

3º - Escolher um aleatório $g \in GF(p^h)$, sendo g um gerador multiplicativo de $GF(p^h)$. Isso será feito escolhendo-se, aleatoriamente, $r \in GF(p^h)$ que satisfaça a condição $r^{(p^h-1)/s} \neq 1$ (para todos os fatores s de p^h-1). Deve ser observado que neste sistema p^h-1 terá apenas divisores primos pequenos, e então é fácil verificar que um dado r satisfaz a condição acima.

Como a densidade de tais geradores é relativamente alta em todos os casos (desprezando qualquer propriedade especial de p e h), o procedimento acima é viável.

4º - Construção de uma mochila segundo o Teorema IV-6 (Teorema de Bose-Chowla), calculando :

$$a_i = \log_g (t + i) \quad , \quad i=0,1,\ldots,p-1 \qquad \text{(IV-180)}$$

5º - Permutar os elementos a_i usando uma permutação π .
Seja $\pi : \{ 0, 1,\ldots,p-1 \} \to \{ 0, 1,\ldots,p-1\}$ uma permutação aleatória escolhida.
Fazer :

$$b_i = a_{\pi(i)} \quad , \quad i=0,1,\ldots,p-1$$

6º - Acrescentar algum ruído à seqüência $b = (b_0,\ldots,b_{p-1})$.
Escolher, aleatoriamente, d tal que $0 \leq d \leq p^h - 2$.
Fazer :

$$C_i = b_i + d \quad , \quad i=0,1,\ldots,p-1 \qquad \text{(IV-181)}$$

7º - Publicar :

$C = (C_0, C_1,\ldots, C_{p-1})$, chave de cifrar ;

e os parâmetros : p , h

8º - Manter secretos : t , g , d , π^{-1}

NOTA : Todos os usuários podem usar o mesmo par de valores p e h . A probabilidade de colisões (dois usuários terem as mesmas chaves) é desprezível.

- CIFRAÇÃO

Para cifrar uma mensagem binária $X = (x_0,\ldots,x_{p-1})$ de tamanho p (tamanho de um vetor é o número de elementos deste vetor) e peso exatamente h (peso é o número de elementos não-nulos), o usuário deve somar todos os elementos C_i da chave pública cujo bit correspondente na mensagem seja 1(um):

$$E(X) = (C_{i_1} + C_{i_2} + \ldots + C_{i_h}) \pmod{p^h-1} \qquad \text{(IV-182)}$$

O valor obtido é o criptograma a ser transmitido.

- DECIFRAÇÃO

O processo de decifração consiste dos seguintes passos:

1º - Seja $r(t) = t^h \bmod f(t)$ um polinômio de grau menor ou igual a h-1 (calculado uma vez na geração do sistema).

2º - Dado : $S = E(X)$, calcular :

$$S' = S - h.d \pmod{p^h-1} \qquad \text{(IV-183)}$$

3º - Calcular $q(t)$, um polinômio de grau h-1 na variável t :

$$q(t) = g^{S'} \bmod f(t) \qquad \text{(IV-184)}$$

4º - Calcular $S(t)$, um polinômio de grau h em GF(p)[t] :

$$S(t) = t^h + q(t) - r(t) \qquad \text{(IV-185)}$$

5º - Tem-se então :

$$S(t) = (t+i_1) . (t+i_2) .... (t+i_h) \qquad \text{(IV-186)}$$

o que significa que $S(t)$ é fatorado em termos lineares sobre GF(p).

Por tentativas sucessivas determinam-se as h raízes i_j. (No máximo p tentativas são necessárias : 0 a p-1 , as possíveis raízes do polinômio.)

6º - Aplicar $\P^{-1}$ para recuperar as coordenadas da mensagem original $X = (x_0, x_1, \ldots, x_{p-1})$ contendo o bit 1(um).

- OBTENÇÃO DE CADEIAS DE BITS ADEQUADAS

Até agora foi suposto que o espaço das mensagens X continha apenas vetores de tamanho p e peso h . Entretanto, os textos binários regulares não apresentam esta forma , sendo, então, necessário aplicar um procedimento para obter textos binários adequados para serem usados pelo criptossistema.

Dado um texto binário, primeiramente, deve-se quebrá-lo em blocos de $\lfloor \log_2 \left\{ \begin{matrix} p \\ h \end{matrix} \right\} \rfloor$ bits cada um , onde :

$$\left\{ \begin{matrix} p \\ h \end{matrix} \right\} = \frac{p!}{h!\,(p-h)!}$$

Cada bloco é visto como uma representação binária de um número n , $0 \leq n < \left\{ \begin{matrix} p \\ h \end{matrix} \right\}$.

Para mapear esses números em vetores binários de peso h , é utilizado o mapeamento de preservação de ordem, que mantém a ordem lexicográfica dos vetores e a ordem natural dos inteiros. Isto é, o mapeamento é tal que a transformação de um número n_a gera um vetor binário y_a , e de um número n_b gera um vetor binário y_b , de modo que se $n_a < n_b$, então, $y_a <\cdot\ y_b$ (onde o símbolo $<\cdot$ indica precedência lexicográfica).

Para dois vetores: $y_a = (y_{a_1}, \ldots, y_{a_p})$ e

$y_b = (y_{b_1}, \ldots, y_{b_p})$

define-se a precedência lexicográfica entre os mesmos como:

- Se $y_{a_1} < y_{b_1}$, então y_a é menor que y_b : ($y_a <\cdot\ y_b$)
- Se $y_{a_i} = y_{b_i}$, i=1,...,k-1 e $y_{a_k} < y_{b_k}$, então y_a é menor que y_b : ($y_a <\cdot\ y_b$)

Se n for maior que $\left\{ \begin{matrix} p-1 \\ h \end{matrix} \right\}$, então o primeiro bit no vetor correspondente será igual a 1(um). Caso contrário, o primeiro bit será o(zero). Atualizam-se, então, os valores de p e h , e fazem-se p iterações, até que todos os p bits sejam determinados.

- Obtenção de um vetor binário y a partir de um número n

Entrada : n , p , h

Saída : $y = (y_1,\ldots,y_p)$

1. PARA i = 1,2,...,p FAÇA
2. SE $n \geq \left\{ \begin{matrix} p-i \\ h \end{matrix} \right\}$ ENTÃO :
3. $y_i \leftarrow 1$
4. $n \leftarrow n - \left\{ \begin{matrix} p-i \\ h \end{matrix} \right\}$
5. $h \leftarrow h - 1$
6. SENÃO $y_i \leftarrow 0$
7. PARE . OBTIDO O VETOR $y = (y_1,\ldots,y_p)$

- Obtenção de um número n a partir de um vetor binário y

Entrada : $y = (y_1,\ldots,y_p)$, p , h

Saída : n

1. $n \leftarrow 0$
2. PARA i = 1,2,...,p FAÇA
3. SE $y_i = 1$ ENTÃO :
4. $n \leftarrow n + \left\{ \begin{matrix} p-i \\ h \end{matrix} \right\}$
5. $h \leftarrow h - 1$
6. PARE . OBTIDO O NÚMERO n

- DESEMPENHO DO CRIPTOSSISTEMA

Segundo avaliação dos próprios autores, o criptossistema mostrado em [55] apresenta o seguinte desempenho :

TEMPO DE PROCESSAMENTO

Cifração : Dada uma mensagem binária de tamanho p e peso h, a cifração equivale a somar h inteiros C_i, cada um menor que p^h.

Decifração : Para decifração são necessárias, aproximadamente, $4.h^3 \log_2 p$ operações em GF(p). Para os parâmetros $p \cong 200$ e $h \cong 25$, são necessárias mais ou menos 500.000 operações em GF(p), o que compara favoravelmente este sistema com o tempo de cifração / decifração do sistema RSA.

TAMANHO DA CHAVE PÚBLICA

O tamanho da chave pública é de p elementos, cada um com valores no intervalo $[\ 1,\ p^h-1\ ]$. Em termos de bits é: $p.\log_2 p^h = p.h \log_2 p$ bits, o que, para o sistema com $p \cong 200$ e $h \cong 25$, fornece uma chave com menos de 40.000 bits. Apesar desse número ser cerca de 35 vezes maior que o tamanho proposto para a chave pública do sistema RSA, ainda está dentro dos limites práticos.

TAXA DE INFORMAÇÃO

A taxa de informação é definida como $R = \log_2 |X| / N$, onde $|X|$ é o tamanho do espaço de mensagem (número de mensagens diferentes), e N é o número de bits no criptograma. Como X pode possuir valores sobre todos os vetores binários de tamanho p e peso h, isto é, $|X| = \left\{ \begin{matrix} p \\ h \end{matrix} \right\}$ e definindo $N = \log_2 p^h$, então :

$$R = \left(\log_2 \left\{ \begin{matrix} p \\ h \end{matrix} \right\} \right) / \left(\log_2 p^h \right) \qquad \text{(IV-187)}$$

- PARÂMETROS PROPOSTOS

A principal dificuldade para implementar o criptossistema proposto é o cálculo de logaritmos discretos em corpos finitos grandes $GF(p^h)$. Este problema computacional, em geral, é considerado muito difícil. No entanto, a escolha adequada dos parâmetros p e h possibilita o emprego de algoritmos conhecidos, e fáceis de serem utilizados, que calculam logaritmos discretos em corpos finitos grandes.

As sugestões apresentadas em [55] para os valores dos parâmetros são :

- $p = 197$, $h = 24$
- $p = 211$, $h = 24$
- $p = 243 = 3^5$, $h = 24$
- $p = 256 = 2^8$, $h = 25$

  (Este caso tem a vantagem do corpo finito ser de característica 2 , permitindo a utilização de aritmética binária tanto no processo de geração de chave como nos cálculos de decifração, além de propiciar implementações mais fáceis.)

  (Característica de um Corpo Finito é definida como sendo o número de 1's que precisam ser somados para obter-se 0(zero).)

Para os parâmetros propostos : $p = 197$, $h = 24$, o sistema apresenta a seguinte taxa de informação , conforme (IV-187) :

$$R = 0.556 \quad ,$$

o que caracteriza uma expansão de dados de 1,798 (= 1/0.556), isto é, uma expansão de dados de aproximadamente 80%.

IV.2.4.2.2 - COMENTÁRIOS

O sistema criptográfico de chave pública proposto por CHOR e RIVEST [55] é baseado no cálculo de logaritmos discretos em Corpos Finitos, e também utiliza o conceito de polinômio irredutível.

No sistema apresentado em [55], a chave pública de cifrar obtida é uma mochila de alta densidade, usando o Teorema de Bose e Chowla.

Os processos de cifração e de decifração, em alguns aspectos semelhantes aos do SCMH, são executados rapidamente, seguindo algoritmos fáceis. A cifração é executada em tempo linear e a decifração, um pouco mais lenta, é rápida quando comparada com o esquema RSA.

A geração da chave de cifrar é a parte mais difícil do sistema proposto. A principal dificuldade para sua implementação reside no cálculo de logaritmos discretos em Corpos Finitos grandes, exigindo uma escolha adequada dos parâmetros que permitam este cálculo.

Uma desvantagem deste criptossistema é a expansão de dados, cerca de 80% (oitenta porcento).

O sistema proposto em [55] permite a incorporação de ruído para aumentar a segurança do método, e admite também cifrar mensagens não-binárias.

Devido às características de construção do sistema proposto, pode-se perceber que os ataques de recuperação da informação "trapdoor" [25], [27] e [29] não se aplicam, pois o sistema não utiliza seqüências supercrescentes.

Também, por gerar mochilas densas,o sistema tem condição de resistir aos ataques a mochilas de baixa densidade [35] e [43].

Quanto aos ataques por reduções sucessivas [6], [21] e [26], nada se pode garantir.

O ataque proposto por ODLYZKO [40] a mochilas multiplicativas não se aplica ao criptossistema que utiliza logaritmos discretos em Corpos Finitos.

O método proposto por KUROSAWA, ITOH, SHIGETA e TSUJII [59] para ataque a criptossistemas de chave pública tipo mochila multiplicativa baseados em Corpos Finitos, não chega a se constituir numa ameaça ao sistema de CHOR e RIVEST[55], porque este ataque somente funciona se o vetor mochila pública possuir três elementos cujos valores forem próximos um do outro, ou se o polinômio primitivo for conhecido. Desta forma , para fugir a este ataque, basta evitar essas condições.

Deve-se ressaltar que o cálculo de logaritmos discretos em Corpos Finitos grandes é um problema difícil, mas o fato de que os parâmetros devem ser escolhidos de forma a permitir que o usuário seja capaz de executar este cálculo pode se constituir numa fraqueza criptoanalítica.

IV.2.4.3 - TEORIA DO CÓDIGO DE CORREÇÃO DE ERRO

Em 1986 NIEDERREITER [56] apresentou um criptossistema mochila de chave pública baseado nos conceitos da Teoria Algébrica da Codificação.

A formulação do criptossistema proposto é apresentada a seguir.

IV.2.3.1 - CONCEITUAÇÃO BÁSICA

Segundo a Teoria Algébrica da Codificação, um código linear C (n,k) sobre o corpo finito F_q de ordem q (isto é, o corpo possui q elementos) é um subespaço linear k-dimensional do espaço vetorial n-dimensional F_q^n sobre F_q , onde $1 \leq k < n$. Assim, C contém, exatamente, q^k palavras-código (no espaço vetorial F_q^n existem q^n seqüências, mas somente q^k são palavras-código).

Para um vetor linha $Y \in F_q^n$ é definido o peso w(Y) como o número de coordenadas não-nulas de Y , e para $X , Y \in F_q^n$ define-se $d(X,Y) = w(X-Y)$ como a distância de "Hamming" (que representa o número de posições em que não há coincidência entre as coordenadas dos vetores X e Y).

A distância mínima do código C é definida como o menor peso de uma palavra-código não-nula de C .

Seja t um inteiro positivo; então diz-se que C tem a capacidade de corrigir t erros se, para qualquer $Y \in F_q^n$, existe, no máximo, um vetor $c \in C$ tal que $d(Y,c) \leq t$.
Se C apresenta uma distância mínima d, então a maior capacidade t de correção de erros de C é $t = \lfloor (d-1)/2 \rfloor$, o que equivale a : $d \geq 2.t + 1$.

O criptossistema de chave pública tipo mochila proposto por NIEDERREITER [56] utiliza, como protótipo, um criptossistema convencional.

Para definir um criptossistema convencional é necessário executar o seguinte procedimento :

1º - Escolha um código linear $C(n,k)$ sobre F_q, que tenha capacidade de corrigir t erros. (Um código adequado é o conhecido Código de Goppa, mas existem outros).

2º - Seja H a matriz de verificação de paridade de C, isto é, H é uma matriz de dimensão $(n-k) \times n$ sobre F_q, de posto $n-k$, tal que C consiste, exatamente, de todas as seqüências $c \in F_q^n$ com $H.c^T = 0$ (onde o índice T significa "transposto").
Na linguagem da Teoria Algébrica da Codificação $H.Y^T$ é a síndrome de Y em relação ao código C.
O criptossistema depende do simples, porém crucial, fato de que a matriz H fornece uma transformação de F_q^n em F_q^{n-k} que é injetiva quando restrita a vetores em F_q^n de peso menor ou igual a t.

Se $H.Y^T = H.Z^T$ para algum Y, $Z \in F_q^n$ com $w(Y) \leq t$ e $w(Z) \leq t$, então $Y = Z$. Isso significa que, se os dois vetores têm a mesma síndrome e possuem peso menor ou igual a t, então estes vetores são iguais. Esta propriedade permite a decodificação única.

3º - Mantenha secreta a matriz H e cifre uma mensagem $Y \in F_q^n$ de peso menor ou igual a t como o criptograma :

$$S = H \cdot Y^T \qquad \text{(IV-188)}$$

4º - Para decifrar, univocamente, o criptograma e recuperar a mensagem Y, o receptor aplica algum algoritmo de decodificação de C à síndrome $H.Y^T$. Como $d(Y,0) = w(Y) \leq t$, então a seqüência Y pode ser vista como um vetor de erros relativo à palavra-código 0 (seqüência nula).

Para obter um criptossistema de chave pública a partir do criptossistema convencional, NIEDERREITER [56] propôs utilizar uma versão modificada da matriz H como sendo a chave pública de cifrar. A técnica usada para modificar a matriz H consiste dos seguintes passos :

1º - Pré-multiplicar a matriz H por uma matriz M aleatória não-singular de dimensão (n-k) x (n-k) sobre F_q .

2º - Pós-multiplicar a matriz resultante por uma outra matriz P aleatória de dimensão n x n sobre F_q , que é obtida pela permutação de linhas de uma matriz diagonal não-singular.

3º - As matrizes M , H e P são mantidas secretas .

4º - A matriz K de dimensão (n-k) x n, resultante do produto matricial, é a chave pública de cifrar do criptossistema:

$$K = M \cdot H \cdot P \qquad \text{(IV-189)}$$

Se M e P forem matrizes identidades de ordem (n-k) e n , respectivamente, a equação (IV-189) gerará uma matriz K de dimensão (n-k) x n.

Para cifrar uma mensagem $Y \in F_q^n$ de peso menor ou igual a t , o usuário deve calcular o criptograma da forma :

$$S = K \cdot Y^T \qquad \text{(IV-190)}$$

Desta forma, os criptogramas são vetores-coluna sobre F_q de tamanho n-k .

Para decifrar o criptograma, o receptor deve executar os seguintes passos :

1º - Pré-multiplicar o criptograma $K.Y^T = M.H.P.Y^T$ pela matriz inversa de M (isto é, M^{-1}) .

2º - Após a multiplicação, obtém-se $H.P.Y^T = H.(Y.P^T)^T$. Note-se que $Y.P^T$ é ,de novo, um vetor de peso menor ou igual a t . Consequentemente, pode-se obter $Y.P^T$ pelo mesmo método usado no criptossistema convencional, por exemplo, aplicando um algoritmo de decodificação de C .

3º - Pós-multiplicando $Y.P^T$ por $(P^T)^{-1}$, recupera-se a mensagem original Y .

Para o caso binário, q=2 , este criptossistema corresponde ao esquema mochila clássico. O criptograma $K.Y^T$ é, então, a soma de, no máximo, t vetores-coluna da matriz chave pública K , e determinar Y é equivalente a decidir quais vetores-coluna de K fornecem a soma dada $K.Y^T$.

Para um valor geral q , o criptograma $K.Y^T$ é uma combinação linear de, no máximo, t vetores-coluna de K , com coeficientes em F_q , e recuperar Y é equivalente a determinar esta combinação linear explicitamente.

A escolha de um código C , adequado para os propósitos do criptossistema proposto, deve considerar os seguintes fatores :

1 - O código C deve ter uma capacidade de correção de erro relativamente grande (ou, equivalentemente, deve ter uma grande distância relativa d/n) para que possa ser usado um número razoável de vetores-mensagem.

2 - O código C deve permitir um algoritmo de decodificação eficiente, de modo que a decifração possa ser executada em um tempo de processamento pequeno.

3 - A dimensão k de C deve ser um valor médio relativo ao tamanho n . Para k muito pequeno existem, relativamente, poucos códigos bons de dimensão k , o que torna mais fácil quebrar o criptossistema. Por outro lado, se k for muito próximo de n , então os criptogramas serão pequenos, o que pode prejudicar a segurança do criptossistema.

IV.2.4.3.2 - COMENTÁRIOS

O sistema criptográfico de chave pública proposto por NIEDERREITER [56] é baseado nas técnicas da Teoria Algébrica de Codificação, apresentando muitas semelhanças com o sistema de McELIECE [58].

O sistema apresentado em [56] pode ser usado para cifração tanto de mensagens binárias como de mensagens não-binárias.

Os ataques possíveis ao criptossistema proposto por Niederreiter podem ser dirigidos contra dois alvos : ou a decifração de um criptograma específico sem o conhecimento das chaves secretas, ou a forma mais ambiciosa de determinar as chaves secretas M , H e P . Esta última tarefa é complicada pelo fato de que a "fatoração" K = M.H.P da chave pública pode não admitir um modo único. Isso caracteriza um contraste com o criptossistema RSA, onde a criptoanálise se baseia, pelo menos, na fatoração única dos inteiros.

O criptossistema de NIEDERREITER [56] apresenta muitas semelhanças com aquele proposto por CHOR e RIVEST [55] . Uma delas é que ambos os sistemas tratam com vetores-mensagem de pouco peso, mas o método de Chor e Rivest tem a desvantagem de consumir mais tempo nos processos de geração do sistema, devido ao cálculo de logaritmos discretos. Um outro aspecto que favorece o criptossistema de Niederreiter é apresentar maior taxa de informação de transmissão de mensagens.

Para uma escolha adequada do código a ser usado e dos parâmetros n , k , d e t , o método de Niederreiter pode gerar uma chave pública de, aproximadamente, 8 Kbits, o que compara este sistema favoravelmente com o método de Chor e Rivest, onde a chave pública é da ordem de 35 Kbits.

Um comentário importante a ser ressaltado é que nem sempre a matriz resultante da multiplicação M.H.P é "difícil" e, portanto, não se pode garantir que o criptossistema será seguro sempre.

Uma sugestão a ser dada aqui, quanto à escolha da matriz M, é que não haja obrigatoriedade desta matriz ser quadrada, bastando apenas possuir inversa à esquerda, pois desta forma, pelo menos, esconde informação quanto ao tamanho da matriz H utilizada.

Quanto à segurança do criptossistema de Niederreiter, pode-se afirmar que a ele não se aplicam os ataques de recuperação da informação "trapdoor" [25], [27] e [29], uma vez que não utiliza seqüências supercrescentes nem transformações modulares.

Nada se pode garantir, no entanto, em relação aos ataques por reduções sucessivas [6], [21] e [26], nem aos ataques a mochilas de baixa densidade [35] e [43].

CAPÍTULO V

CONCLUSÕES E OBSERVAÇÕES

A criptografia tem adquirido, recentemente, grande importância como meio de proteger informações em computadores e em sistemas de comunicações. Por isso, atividades de pesquisa em criptografia têm aumentado, ultimamente, em resposta à necessidade de se obterem formas seguras para proteger a integridade de dados sensíveis durante sua geração (criação) , armazenamento e transmissão.

Os sistemas eletrônicos de comunicação oferecem velocidade, precisão e diminuem os custos envolvidos, mas eles também apresentam sérios problemas de segurança, pois estes sistemas são susceptíveis a interceptações e falsificações . Uma maneira de prevenir intervenções impróprias nos novos sistemas eletrônicos e proteger a grande quantidade de informações privadas (como registros de crédito, históricos médicos, etc..., agora armazenados em bancos de dados em computador) é recorrer às técnicas criptográficas.

Dentre os métodos criptográficos recentes está o criptossistema de chave pública baseado no problema da mochila. Desenvolvido em 1978 por MERKLE e HELLMAN [3], este esquema de cifração e decifração é simples e muito prático, tendo sido considerado, até 1982, como "altamente seguro" [4] e [7], porque as melhores técnicas para resolver problemas mochila pareciam ser de complexidade computacional exponencial.

Em 1982 SHAMIR [27] apresentou, com sucesso, um ataque eficaz contra o sistema básico de Merkle-Hellman, propondo um método para resolver, em tempo polinomial, criptossistemas mochila de iteração simples que utilizam seqüências supercrescentes. Este trabalho de criptoanálise do SCMH teve grande repercussão e caracterizou a insegurança dos criptossistemas mochila cuja chave pública é gerada a partir de seqüência supercrescente usando transformação modular.

O esquema de iteração múltipla de Merkle-Hellman foi considerado seguro até que DESMEDT et alii [38] mostraram que o uso de várias transformações modulares não garante uma segurança maior para o criptossistema, uma vez que a chave de cifrar obtida por transformações modulares iterativas pode também ser quebrada [21],[26] e [33]. Em 1983 foi, então, proposto por ADLEMAN [34] um método de quebra específico para o sistema de Merkle-Hellman de iteração múltipla.

Uma formulação diferente para criptoanálise dos sistemas criptográficos tipo mochila é o ataque a mochilas de baixa densidade proposto por BRICKELL [35] e por LAGARIAS-ODLYZKO [43]. O ponto mais interessante sobre este tipo de ataque é que não é feita nenhuma suposição sobre o modo de construção do sistema e, assim, pode ser aplicável a qualquer criptossistema mochila (diferentemente do ataque de Shamir que se baseia fortemente na existência de seqüência supercrescente). Um resultado desses ataques é mostrar que os criptossistemas mochila de chave pública, que possuem baixa densidade, podem ser considerados como inseguros.

Com base nos estudos referenciados no presente trabalho, pode-se afirmar que, por muitas razões, a segurança do criptossistema mochila original, proposto por MERKLE e HELLMAN [3], foi considerada altamente exagerada até o aparecimento dos ataques criptoanalíticos bem sucedidos.

A vulnerabilidade criptoanalítica do SCMH é devida às seguintes características :

- A idéia principal do criptossistema mochila de chave pública é transformar um problema "fácil" em um problema "difícil", mantendo secretos os parâmetros dessa transformação . Do ponto de vista do criptoanalista, um método para quebrar o sistema é construir a mochila fácil original a partir da mochila difícil pública. Merkle e Hellman afirmaram que este método exaustivo não é prático. No entanto, o criptoanalista não precisa ter a seqüência supercrescente original para quebrar o esquema : basta determinar uma chave de decifrar "fácil", usando uma transformação modular.

- Até agora já é bem sabido que chaves de cifrar, obtidas após uma única transformação de seqüência supercrescente, podem ser usualmente quebradas [27]. Desta forma, uma pessoa pode querer construir chaves de cifrar seguras utilizando muitas transformações [3]. Entretanto, transformações iterativas não garantem uma segurança maior [21] e [38]. Usando transformações iterativas três casos são possíveis :
  1º - A segurança é completamente perdida (por exemplo, obtém-se outra vez uma seqüência supercrescente);
  2º - O mesmo nível de segurança é obtido, como se apenas uma transformação tivesse sido feita (por exemplo, a chave de cifrar pode ser convertida, por uma transformação, em uma seqüência supercrescente - não necessariamente a seqüência supercrescente original);
  3º - Uma segurança maior é obtida.

- Mesmo sabendo-se que o vetor público foi gerado a partir de um vetor supercrescente,pode-se tentar explorar outras propriedades a fim de quebrar a cifra. Tais propriedades podem permitir quebrar 1 (um) bit do texto claro. Algumas vezes é fácil determinar alguns bits, enquanto é difícil determinar todos os bits do texto claro. Devido à redundância, alguns bits podem revelar muita informação. Por isso, para propósitos criptoanalíticos, a busca por uma transformação em uma seqüência supercrescente pode ser relaxada simplesmente pela busca por uma transformação tal que 1 (um) bit da mensagem binária possa ser determinado facilmente.

A fim de responder à questão se a mochila serve ou não para ser usada como um sistema criptográfico seguro, isto é, se este sistema tem condição de resistir a todos os ataques conhecidos (mesmo impondo algumas restrições) ou, equivalentemente, se existe alguma maneira de contornar esses ataques, são necessários ainda muitos estudos.

No Capítulo III foram ressaltados os aspectos que podem tornar viáveis as tentativas de quebra do sistema de chave pública tipo mochila, evidenciando, de certa forma, as medidas alternativas que podem ser utilizadas para contornar tais vulnerabilidades visando a tornar algum algoritmo mochila mais seguro às investidas criptoanalíticas. Com a finalidade de obter maior sucesso na tarefa de criptoanálise, pode ser utilizada, quando possível, uma combinação dos ataques apresentados no capítulo mencionado.

O ataque por reduções sucessivas, se funcionar sempre, parece ser o método mais aplicável às formulações descritas. Assim, se os ataques por reduções sucessivas (para obter uma seqüência com elemento dominante) forem bem mais eficientes que o método de força bruta, então isso poderá significar que a mochila como sistema criptográfico terá chegado ao fim, mas isso precisa ser provado formalmente.

Como reação natural aos ataques criptoanalíticos propostos para quebrar os sistemas criptográficos de chave pública tipo mochila, vários autores, na tentativa de "salvar" estes criptossistemas, apresentaram novas formulações como forma de superar estes ataques. Estas formulações foram mostradas no Capítulo IV, onde podem ser observadas as características necessárias para um sistema seguro, evitando-se aquelas condições que viabilizam os ataques criptoanalíticos.

É claro que, para determinar qual o melhor sistema criptográfico de chave pública tipo mochila, é preciso haver um compromisso entre segurança e simplicidade, isto é, o melhor sistema é aquele que além de resistir à maioria dos ataques criptoanalíticos conhecidos, deve também possuir processos rápidos de cifração e decifração.

Com as novas formulações apresentadas neste trabalho, o algoritmo mochila poderá resistir a muitos tipos de ataques criptoanalíticos, até que o avanço da tecnologia force a sua revisão.

A elegância e simplicidade de muitos dos recentes esquemas de chave pública não deve fazer com que os estudiosos no assunto adotem um sentimento de satisfação e acomodação. O trabalho que precisa ser feito nesta nova e excitante área de pesquisa apenas começou. O que ainda é necessário são novas medidas de complexidade especialmente definidas para o problema de criptoanálise. Quando for possível garantir a segurança de criptossistemas de acordo com tais medidas de criptocomplexidade, então o problema da segurança de comunicação estará resolvido. Os sistemas criptográficos de chave pública baseados no problema da mochila devem continuar sendo discutidos e analisados até que possa ser provado formalmente se esse tipo de criptossistema é seguro ou não do ponto de vista criptográfico.

À luz dos diversos ataques criptoanalíticos apresentados, poderia parecer que o criptossistema mochila de chave pública teria chegado ao seu fim. Afirmar que um criptoalgoritmo, para uma particular escolha de chave, pode ser criptoanalisado em tempo polinomial, não é sinônimo de que o mesmo não seja seguro. Por exemplo, o algoritmo de Shamir, descrito em [27], apesar de polinomial no tempo, é muito lento a ponto de torná-lo computacionalmente inviável para criptoanalisar mochilas de algumas centenas de elementos, enquanto a dificuldade computacional para cifrar e decifrar criptossistemas mochila deste tamanho é inteiramente viável. O mesmo pode acontecer com os demais ataques criptoanalíticos apresentados.

Além disso, outros autores preocupados com a segurança do criptossistema mochila de chave pública sugeriram mudanças na formulação original a fim de torná-lo mais seguro.

Assim sendo, ainda não se pode provar que o criptossistema de chave pública tipo mochila não tenha mais aplicações criptográficas...

O presente trabalho teve por finalidade dar conhecimento dos conceitos sobre sistemas criptográficos de chave pública tipo mochila (apresentando suas aplicações práticas) e realizar um estudo comparativo dos diversos ataques aos criptossistemas mochila de chave pública e também das diversas formulações destes sistemas. Foi dado um enfoque mais abrangente e, por conseguinte, mais superficial, sendo necessárias investigações mais profundas e detalhadas sobre alguns pontos de maior interesse. No entanto, este trabalho deve servir para despertar a curiosidade dos leitores e estudiosos sobre o assunto, a fim de estimular a elaboração de trabalhos futuros nesta área, servindo a presente tese como base e ponto de partida.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] DIFFIE, W.; HELLMAN, M. : "New Directions in Cryptography", IEEE Transactions on Information Theory, vol. IT-22, nº 6, pp. 644-654, November 1976.

[2] RIVEST, R.; SHAMIR,A.; ADLEMAN, L. : "A Method for Obtaining Digital Signatures and Public-Key Cryptosys tems", CACM, vol. 21, nº 2, pp. 120-126, February 1978.

[3] MERKLE, R.; HELLMAN, M. : "Hiding Information and Signatures in Trapdoor Knapsack", IEEE Transactions on Information Theory, vol. IT-24, nº 5, pp. 525-530 , September 1978.

[4] HELLMAN, M. : "The Mathematics of Public-Key Cryptography", Scientific American, vol. 234, nº 8, pp. 146-157, August 1979.

[5] HELLMAN, M. : "An Overview of Public-Key Cryptography", IEEE Communications Society Magazine, vol. 16, nº 6, pp. 24-32, November 1978.

[6] HERLESTAM, T. : "Critical Remarks on Some Public Key Cryptosystems", BIT, vol. 18, pp. 493-496, 1978.

[7] DIFFIE, W.; HELLMAN, M. : "Privacy and Authentication : An Introduction to Cryptography", Proceedings of the IEEE, vol. 67, nº 3, pp. 397-427, March 1979.

[8] DAVIES, D.W.; PRICE, W.L.; PARKIN, G.I. : "Evaluation of Public-Key Cryptosystems", IPC Business Press, vol. 2, nº 4, pp 138-154, July 1980.

[9] SHAMIR, A. : "On the Cryptocomplexity of Knapsack Systems", Proceedings of Symp. ACM Theory Comput., vol. 11, pp. 118-129, 1979.

[10] WILLETT, M. : "Deliberate Noise in a Modern Cryptographic System", IEEE Transactions on Information Theory, vol. IT-26, nº 1, pp. 102-105, January 1980.

[11] MILLER, D.V. : "Ciphertext only Attack on the Merkle-Hellman Public-Key System Under Broadcast Situations", Cryptologia, vol. 6, nº 3, pp. 279-281, July 1982.

[12] ARAZI, B. : "A Trapdoor Multiple Mapping", IEEE Transactions on Information Theory, vol. IT-26, nº 1 , pp. 100-102, January 1980.

[13] SHAMIR, A.; ZIPPEL, R.E. : "On the Security of the Merkle-Hellman Cryptographic Scheme", IEEE Transactions on Information Theory, vol. IT-26, nº 3, pp. 339-340, May 1980.

[14] AMIRAZIZI, H.; KARNIN, E.; REYNERI,J. : "A Polinomial Time Solution for Compact Knapsacks", Advances in Cryptography - A Report on CRYPTO-81, pp.1-3, Allen Gersho Editor, Santa Barbara, California,1981.

[15] INGEMARSSON, I. : "Some Comments on the Knapsack Problem - Are all Injective Knapsack Partly Solvable after Multiplication Modulo Q ?", Advances in Cryptography - A Report on CRYPTO-81, pp. 20-24, Allen Gersho Editor, Santa Barbara, California, 1981.

[16] HENRY, P.S. : "Fast Decryption Algorithm for the Knapsack Cryptographic System", Bell System Technical Journal, vol. 60, nº 5, pp. 767-773, May-June 1981.

[17] DESMEDT, Y.; VANDEWALLE, J.; GOVAERTS, R. : "Linear Algebra and Extended Mappings Generalize Public Key Cryptographic Knapsack Algorithms", Electronics Letters, vol. 19, nº 10, pp. 379-381, 12th May 1983.

[18] GOODMAN, R. : "Processing Techniques in Public Key Cryptosystems", Cryptography, Section 4.3, pp. 465-476 , 1982.

[19] BRICKELL, E.F. : "A New Knapsack-Based Cryptosystem" , Sandia National Laboratories, Albuquerque, New Mexico, USA, 87185, pp. 1-8, 1983.

[20] WILLIANS, H.C. : "Computationally "HARD" Problems as a Source for Cryptosystems", Secure Communication and Asymmetric Cryptosystems, AAAS Selected Symposia Series, Westview Press, Inc., Colorado, 1982.

[21] DESMEDT, Y.; VANDEWALLE, J.; GOVAERTS, R. : "How Iterative Transformations can help to crack the Merkle-Hellman Cryptographic Scheme", Electronics Letters, vol. 18, nº 21, pp. 910-911, 14 October 1982.

[22] MERKLE, R.C. : "Secure Communication over Insecure Channels", Commun. ACM, vol. 21, nº 4, pp. 294-299 , April 1978.

[23] SIMMONS, G.J. : "Symmetric and Asymmetric Encryption" , Secure Communication and Asymmetric Cryptosystems , AAAS Selected Symposia Series, Westview Press, Inc., Colorado, 1982.

[24] DIFFIE, W. : "Conventional versus Public Key Cryptosystems", Secure Communication and Asymmetric Cryptosystems, AAAS Selected Symposia Series, Westview Press, Inc., Colorado, 1982.

[25] EIER, R.; LAGGER, H. : "Trapdoors in Knapsacks Cryptosystems", Cryptography: Lectures Notes in Computer Science, nº 149, pp. 316-322, New York, Springer-Verlag, Berlin, Heidelberg, 1982.

[26] INGEMARSSON, I. : "A New Algorithm for the Solution of the Knapsack Problem", Cryptography: Lectures Notes in Computer Science,nº 149, pp. 309-315, New York , Springer-Verlag, Berlin, Heidelberg, 1982.

[27] SHAMIR, A. : "A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem", IEEE Proceedings of 23rd Annual Symposium on Foundations of Computer Science,pp. 145-152, November 1982.

[28] BRICKELL, E.F.; DAVIS, J.A.; SIMMONS, G.J. : "A Preliminary Report on the Cryptoanalysis of Merkle-Hellman Knapsack Cryptosystems", Advances in Cryptology - Proceedings of CRYPTO-82, Plenum Press, New York and London, 1983.

[29] BRICKELL, E.F.; SIMMONS, G.J. : "A Status Report on Knapsack Public Key Cryptosystems", Congressus Numerantium, vol. 37, pp. 3-72, 1983.

[30] WILLETT, M. : "Trapdoor Knapsack without superincreasing Structure", Information Processing Letters, vol. 17, nº 1, pp. 7-11, 19 July 1983.

[31] POHLIG, S.C.; HELLMAN, M.E. : "An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance", IEEE Transactions on Information Theory, vol. IT-24, nº 1, pp. 106-110, January 1978.

[32] SHAMIR, A. : "Embedding Cryptographic Trapdoors in Arbitrary Knapsack Systems", Information Processing Letters, vol. 17, nº 2, pp. 77-79, 24 August 1983.

[33] ADLEMAN, L.M. : "On Breaking the Iterated Merkle-Hellman Public-Key Cryptosystem", Advances in Cryptology - Proceedings of CRYPTO-82, pp. 303-308, Plenum Press, New York and London, 1983.

[34] ADLEMAN, L.M. : "On Breaking Generalized Knapsack Public Key Cryptosystems", Proceedings of the 15th Annual ACM Symposium on Theory of Computing, pp. 402-412 , 1983.

[35] BRICKELL, E.F. : "Solving Low-Density Knapsacks". Advances in Cryptology - Proceedings of CRYPTO-83,pp. 25-37, Plenum Press, New York and London, 1984.

[36] LAGARIAS, J.C. : "Knapsack-Type Public Key Cryptosystems and Diophantine Approximation", Advances in Cryptology - Proceedings of CRYPTO-83, pp. 3-23, Plenum Press, New York and London, 1984.

[37] DESMEDT, Y.; VANDEWALLE, J.; GOVAERTS, R. : "The Most General Cryptographic Knapsack Scheme", Carnahan Conference on Security Technology, University of Kentucky, Kentucky, Lexington, pp. 115-120, May 1984.

[38] DESMEDT, Y.; VANDEWALLE, J.; GOVAERTS ,R. : "Critical Analysis of the Security of Knapsack Public-Key Algorithms", IEEE Transactions on Information Theory, vol. IT-30, nº 4, pp. 601-611, July 1984.

[39] RETKIN, H. : "Multi-level Knapsack Encryption", International Conference on Secure Communication Systems, The Hatfield Polytechnic, Hatfield, England, pp. 48-49, 1984.

[40] ODLYZKO, A.M. : "Cryptoanalytic Attacks on the Multiplicative Knapsack Cryptosystem and on Shamir's Fast Signature Scheme", IEEE Transactions on Information Theory, vol. IT-30, nº 4, pp. 594-601, July 1984.

[41] COOPER, R.; PATTERSON, W. : "A Generalization of the Knapsack Algorithm using Galois Field", Cryptologia , vol. 8, nº 4, pp. 343-347, October 1984.

[42] PIEPRZYK; J.P.; RUTKOWSKI, D.A. : "Design of Public Key Cryptosystems using Idempotent Elements", Technical Academy of Bydgoszcz and Technical University of Gdansk, Poland, pp. 64-68, 1985.

[43] LAGARIAS, J.C.; ODLYZKO, A.M. : "Solving Low-Density Subset Sum Problems", JACM, vol. 32, nº 1, pp. 229-246 , January 1985.

[44] GOODMAN, R.M.F.; McAULEY, A.J. : "New Trapdoor-Knapsack Public-Key Cryptosystem", Advances in Cryptology - Proceedings of EUROCRYPT-84, pp. 150-158, Springer-Verlag, Berlin - Heidelberg - New York - Tokyo, 1985.

[45] DI PORTO, A. : "Un Algoritmo Crittografico a Chiave Pubblica basato su una Generalizzazione del Problema del Knapsack", Note Recensioni e Notizie, vol. XXXIII, Numero 1-2, pp. 41-44, Gennaio-Giugno 1985.

[46] PAZ DE LIMA, A. : "Sistema Criptográfico tipo Mochila usando Seqüência k-supercrescente e Matriz de Difusão", Palestra apresentada no IME, Rio de Janeiro, 1982. (Trabalho não publicado)

[47] PAZ DE LIMA, A. : "Utilização de Mochila Injetiva Não-Supercrescente no Criptossistema de Chave Pública ", Palestra apresentada na UFF, Rio de Janeiro, 1982. (Trabalho não publicado)

[48] LENSTRA Jr., H.W. : "Integer Programming with a Fixed Number of Variables", University of Amsterdam, Dept. of Mathematics, Technical Report, 81-03, pp. 1-20, April 1981.

[49] CASSELS, J.W. : "An Introduction to Diophantine Approximations", Cambridge University Press, Cambridge,1965.

[50] LENSTRA, A.K.; LENSTRA Jr., H.W.; LOVÁSZ, L. : "Factoring Polynomials with Rational Coefficients",Mathematishe Annalen, vol. 261, nº 4, pp. 515-534, 1982.

[51] FRIEZE, A.M. : "On the Lagarias-Odlyzko Algorithm for the Subset Sum Problem", SIAM, vol. 15, nº 2 , pp. 536-539, May 1986.

[52] PAZ DE LIMA, A. : "Utilização de Polinômios Irredutíveis e Multiplicador Matricial nos Sistemas Mochila em Corpos Finitos - Uma Aplicação Prática", Palestra apresentada no INPE, São José dos Campos, 1983. (Trabalho não publicado)

[53] PAZ DE LIMA, A. : "Criptossistema Mochila Utilizando Números Primos e Multiplicador Matricial", Palestra apresentada no IME, Rio de Janeiro, 1984. (Trabalho não publicado)

[54] ITOH, T.; KUROSAWA, K.; TSUJII, S. : "Reliability of Public-Key Cryptosystems using the Knapsack Problem", Electronics and Communications in Japan, Part 1 , vol. 68, nº 9, pp. 45-50, 1985.

[55] CHOR, B.; RIVEST, R.L. : "A Knapsak Type Public Key Cryptosystem based on Arithmetic in Finite Fields", Advances in Cryptology - Proceedings of CRYPTO-84, pp. 54-65, Springer-Verlag, New York, 1985.

[56] NIEDERREITER, H. : "Knapsack-Type Cryptosystems and Algebraic Coding Theory", Problems of Control and Information Theory, vol. 15, nº 2, pp. 159-166, 1986.

[57] BRICKELL, E.F.; LAGARIAS, J.C.; ODLYZKO, A.M. : "Evaluation of the Adleman Attack on Multiple Iterated Knapsack Cryptosystems", Advances in Cryptology - Proceedings of CRYPTO-83, pp.39-42, Plenum Press, New York and London, 1984.

[58] McELIECE, R. : "A Public Key Cryptosystem based on Algebraic Coding Theory", DSN Progress Rep 42-44, Jet Propulsion Lab, California Institute of Technology , Pasadena, California, January-February 1978 .

[59] KUROSAWA, K.; ITOH, T.; SHIGETA, H.; TSUJII, S. : "An Attacking Method for Multiplicative Knapsack Type Public Key Cryptosystem based on Finite Fields" , Transactions of the IEICE, vol. E-70, nº 1, pp. 37-41, January 1987.

[60] KNUTH, D.E. : The Art Of Computer Programming : Volume 2 Semi-Numerical Algorithms, Addison-Wesley, Reading , Mass., 1969.

[61] LE VEQUE, W.J. : Fundamentals of Number Theory, Addison-Wesley, Reading, Mass., 1977.

[62] LINDSAY, C. : A Concrete Introduction to Higher Algebra, Springer-Verlag, New York, Berlin, Heidelberg, 1979.

[63] DENNING, D.E.R. : Cryptography and Data Security , Addison-Wesley Publishing Company Inc., 1982.

[64] BECKER, H.; PIPER, F. : Cipher Systems - The Protection of Communications, Wiley-Interscience Publication , John Wiley and Sons, 1982.

[65] PAPADIMITRIOU, C.; STEIGLITZ, K. : Combinatorial Optimization : Algorithms and Complexity, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1982.