# CRI PTOSISTEMAS DF CHAVE PUBLICA

D ISSERTACÃO

Apresentada ao Mestrado

em Engenharia Elétrica da UFPE

por

FERNANDA M. R. DE ALENCAR

como um dos requisitos para obtenção
do titulo de Mestre

UFPE - RECIFE

1991

**FERNANDA MARIA RIBEIRO DE ALENCAR**

# CRIPTOSISTEMAS DE CHAVE PUBLICA

Dissertação apresentada à Coordenação de Pós-Graduação em Engenharia Elétrica do Centro de Tecnologia da Universidade Federal de Pernambuco, como parte dos requisitos para a obtenção do título de Mestre em Engenharia Elétrica.

Orientador : Ricardo Menezes Campello de Souza

Recife

1991

A DEUS

E

PARA MINHA AVÓ

ADER HA PEREIRA

# AGRADECIMENTOS

Meus agradecimentos são endereçados, acima de tudo a Deus nosso Pai Maior pela oportunidade de uma nova existência e de poder usar os recursos de que me presenteou, e em especial a minha companheira, amiga, mãe e avó, Dona Aderita, pelo incentivo e carinho com que sempre me cercou.

Aos meus pais, onde minha homenagem maior e agradecimento são dedicados, em memória, ao meu pai.

Ao meu orientador, professor e amigo Ricardo Menezes Campello de Souza, pelo incentivo a ingressar na vida acadêmica, e colaboração com energias sempre positivas, dando-me maior tranquilidade e segurança para lutar pelo que acredito.

Ao professor Ascendino Flávio, coordenador da Pós-Graduação, pelo incentivo à conclusão desse trabalho.

Ao companheiro e amigo, José Roberto, pela paciência dispensada nesses últimos momentos de conclusão do trabalho.

A todos os companheiros e amigos que acompanharam todos os momentos de dificuldades, dando-me forças renovadoras positivas, proporcionando-me momentos de alegria.

Enfim, aos demais colegas e amigos do Departamento de Ele

trônica e Sistemas que muito colaboraram, direta ou inderetamente, com o meu enriquecimento profissional e pessoal, em especial a Wander Broell Faria, as amigas Andrea Tenório Pinto, secretária da Pós-Graduação, Ivanice de Brito Galvão, secretária do Departamento, e Adriana Maria Pessoa Leo, e ao amigo Ricardo José Britto Salgueiro pelo incentivo constante.

Rogo ao Pai que retribua a todos o carinho e a energia incentivadora a mim dispensados.

SUMÁRIO

a seleção de chaves de cifragem do algoritmo RSA, fato que permitirá sua constante utilização em inúmeras aplicações cujo objetivo principal é o de garantir a privacidade e a autenticidade das informações.

De forma geral, neste capítulo foi feito um estudo mais detalhado acerca de um algoritmo de chave pública reconhecido plenamente pelo comunidade científica, o algoritmo da mochila com alçapão de Merkle e Hellman. Procurou-se avaliar algumas de suas variações, porém, maior atenção foi dada ao processo de cifragem e decifragem utilizando-se a mochila aditiva binária simples, bem como, ao processo de criptanálise da mesma, proposto por Shamir. Quanto as demais variações da mochila (fig. 3.1), pode-se encontrar maiores detalhes em alguns trabalhos, com por exemplo [6], que constam também de algumas criptanálises.

Ao longo do estudo realizado não se encontrou nenhuma citação a respeito da mochila multinível, exceto a feita por Merkle e Hellman em seu trabalho original [1], tendo-se assim, ao que parece, muito campo a ser explorado.

## REFERÊNCIAS BIBLIOGRÁFICAS

[1] Ralph C. Merkle e Martin E. Hellman, "Hiding Information and Signatures in Trapdoor Knapsacks", IEEE Transactions Information Theory, vol. 24, n. 5, pp. 525-530, Set. 1978.

[2] Whitfield Diffie, "The First Ten Years **of** Public-Key Cryptography ", Proceedings of the IEEE, vol. 76, n. 5, pp. 560-577, Maio 1988.

[3] A. Shamir, **"A** Polynomial-Time Algorithm for Breaking the Basic Merklen-Hellman Cryptosystem", IEEE Transactions on Information Theory, vol. IT-30, n. 5, pp. 699-704, Set. 1984.

[4] E. F. Brickell, "Breaking Iterated Knapsacks", Crypto' 84, pp. 342-358.

[5] Andrew. M. Odlyzko, "Cryptanalytic Attacks on the Multiplicative Knapsack Cryptosystem and on Shamir's Fast Signature Scheme", IEEE Transactions on Information Theory, vol IT-30, n. 4, pp. 594-601, Julho 1984.

[6] Ernest F. Brickell e Andrew M. Odlyzko, "Criptanalysis: **A** Survey **of** Recent Results", Proceedings of the IEEE, vol. 76, n. 5, pp. 578-593, Maio 1988.

[7] A. Shamir e R. Zippel, "On the Security **of** the Merkle-Hellman Cryptographic Scheme", IEEE Transactions on Information Theory, vol. 26, n. 3, pp. 339-340, Maio 1980.

[8] Yvo G. Desmedt, Joos P. Vandewalle e René J. M. Govaerts, "A Critical Analysis of the Security of Knapsack Public-Key Algorithms", IEEE Transactions on Information Theory, vol. IT-30, n. 4, pp. 601-611, Julho 1984.

# CAPITULO IV

## O ALGORÍTMO RSA

Dentre os vários criptosistemas de chave pública, aquele proposto por Rivest, Shamir e Adlmean em 1978, conhecido por RSA [1], parece ainda ser o mais utilizado [2] e o melhor dentre os criptosistemas que utilizam duas chaves [3].

No sistema RSA, utiliza-se o fato de ser menos complexa, computacionalmente, a tarefa de se determinar números primos, em com paração com a fatoração de inteiros [4], [5]. Isso porque esse algo ritmo se fundamenta na escolha de dois números primos grandes, p e q, mantidos em segredo, cujo produto se constituirá no módulo n da operação de cifragem e decifragem das mensagens. Atualmente, o meto do pode ser estendido para o produto de mais de 2 primos, mas parece não haver vantagem em se fazer isso. Para o processo de cifragem é necessário ainda a existência de um inteiro "e" relativamente primo com (p-1)(q-1), que, em conjunto com n, constituirá a chave pública de crifragem (e,n) [3].

Nesse criptosistema, a função unidirecional com alça pão a ser utilizada consiste em uma exponenciação discreta, ou seja, em aritmética modular sobre uma exponenciação de inteiros. Pela natu

reza das transformações envolvidas nesse algoritmo, vê-se que o mesmo poderá ser utilizado tanto na privacidade quanto na autenticação de mensagens, fato este que não ocorre com o algoritmo da mochila.

## 4.1 - DESCRIÇÃO DO ALGORÍTMO

Trata-se de um esquema de cifragem onde uma mensagem clara M é dividida em sucessivos blocos $M_1$, $M_2$, ..., que são cifrados com uma mesma chave, segundo a expressão

$$C_i = E_k(K) = \quad \pmod n \qquad (4.1)$$

onde cada corresponde à parte do texto claro cuja representação numérica está no intervalo [0, n-1]. Vê-se, assim, que a função de cifragem E (.)/ mapeia um espaço em outro semelhante, fato que não se verifica no criptosistema de Merkle-Hellman.

Cada usuário possui uma chave de cifragem pública dada pelo par de inteiros positivos $k_i$ = (e,n) e uma chave de decifragem secreta $K_s$ = (d,n), também um par de inteiros.

A mensagem enviada é recuperada a partir do criptograma C

recebido, também computando-se uma exponenciação

$$(C) = C^{d} \pmod{n} \qquad (4.2)$$

Essa função de decifragem $_{2}(.)$ é semelhante a de cifragem. As transformações de cifragem e decifragem encontram-se baseadas na generalização de Euler para o Teorema de Fermât [A.III], onde se prova que para um M relativamente primo com n, tem-se

$$M^{\phi(n)} = 1 \pmod{n} \qquad (4.3)$$

Além disso, se

$$ed = 1 \pmod{\phi(n)} \qquad (4.4)$$

então essas transformações serão comutativas e inversas. Por essa propriedade, o esquema RSA pode ser utilizado tanto para garantir privacidade como autenticidade em sistemas de chave pública [6].

## 4.2 - PROCEDIMENTO EFICIENTE PARA CIFRAGEM E DECIFRAGEM

Rivest, Shamir e Adleman apresentam, em seu trabalho, um procedimento eficiente onde a determinação do texto cifrado $M^e \pmod n$, requer no máximo $2*\log_2(e)$ multiplicações e $2*\log_2(e)$ divisões.

Procedimento:

Passo 1 : Seja e^, •••• $e_l\ e_0$ a representação binária de e.

Passo 2 : Faça a variável C igual a 1.

Passo 3 : Repetir os passos 3a e 3b para i = k, k-1 ... 0.

Passo 3a : Faça C igual ao resto da divisão de C por n.

Passo 3b : Se = 1, então faça C igual ao resto da divisão de C * M por n.

Passo 4 : Pare. C será a forma cifrada de M.

A decifragem, por ser uma transformação inversa, também

poderá ser feita através desse mesmo procedimento só que utilizando d no lugar de e. Outras rotinas mais eficientes são conhecidas. Na seção 4.4 será apresentada uma rotina eficiente para a decifragem proposta por Quisquater e Couvreur [2]. Tem-se a seguir um exemplo onde se faz uso do algoritmo acima mencionado.

EXEMPLO 4.1

Considere o caso onde se dispõe dos primos p = 47, q = 59 e, portanto, n = pq = 2773, além de e = 17. Desta forma, tem-se que $\phi(n) = (P - 1)(q - 1) = 2668$ e a partir da equação 3.4 que d = 157, o inverso multiplicativo de e (mod $\phi$(n)).

Desde que n = 2773, pode-se codificar duas letras por bloco, substituindo cada letra por um número de 2 digitos, da seguinte forma:

A = 01, B = 02, Z = 26 e ESPAÇO BRANCO = 00

Considere a mensagem

M = É TUDO GREGO PARA MIM

Codificando-a cm blocos de dois caracteres, tem-se

M = 0500 2021 0415 0007 1805 0715 0016 0118 0100 1309 1300

Para os onze blocos em que ficou divida a mensagem aplica se o procedimento que determina o texto cifrado equivalente a cada bloco M , da mesma forma que a transformação expressa pela equação 3.1.

1. Considere o primeiro bloco da mensagem M, 0500 , tem -se

Passo 1: representação binária da chave de cifragem e = 10001 e portanto, k = 4;

Passo 2: **C** =

Passo 3: Para i **0**

i = 4

3a: $C_i$ = resto $e^2$ / n 1 = 1

3b: e = 1, então **C** = resto M / n ] = 500

$M_6 = 0715 \rightarrow C_6 = 1462$

$M_7 = 0016 \rightarrow C_7 = 729$

$M_8 = 0118 \rightarrow C_8 = 1239$

$M_9 = 0100 \rightarrow C_9 = 1952$

$M_{10} = 1309 \rightarrow C_{10} = 840$

$M_{11} = 1300 \rightarrow C_{11} = 446$

O criptograma correspondente a mensagem M é, portanto,

C = 1655 0094 1331 1698 2423 1462 0729 1239 1952 0840 0446

Aplicando-se o mesmo procedimento, so que agora utilizando a expressão 4.2 com d = 157, a cada bloco de quatro caracteres do criptograma recebido, obtem-se a mensagem M enviada.

///

## 4.3 - DETERMINAÇÃO DO MÓDULO n

Como as transformações de cifragem e decifragem são inversas, a obtenção da chave secreta (d,n) e a segurança do esquema

# ABSTRACT

Cryptology is the science that studies the principles and techniques for achieving secure communications over insecure channels and this work is devoted to it. Many aspects of its fundamental branches, cryptography and cryptanalysis, are considered, with emphasis being given to Shannon's information theoretic approach to the field and to the contemporary techniques of public-key encipherment developed by Withfield Diffie and Martin Hellman.

Public-key cryptography was invented in the spring of 1975 and represented a conceptual breakthrough which revolutionized the field of Cryptology and provided an elegant solution to the important problems of key distribution and authentication in large computer networks. In this context, two of the most important publie-key cryptosystems are analysed, the knapsack and the RSA system. Some aspects of the main cryptanalytic atack to the Merkle-Hellman knapsack are presented and a number of factorization methods and primality tests are discussed, as a mean to aid the selection of keys for the RSA algorithm. A few applications of the public-key techniques are described and a list of research topics for future investigation is suggested.

provável primo. Para testar se b é realmente primo são gerados 100 números aleatoriamente distribuídos, a c [1, b-1]. O algoritmo de teste de primalidade considerado foi o de Solovay e Strassen. Testa se, se

$$\text{mdc}(a,b) = 1$$

$$J(a,b) \equiv a^{(b-1)/2} \pmod{b} \tag{4.7}$$

onde J(a,b) é conhecido como simbolo de Jacobi [A.I]. Se o número b for primo as expressões em 4.7 deverão ser verdadeiras para todos os 100 valores escolhidos. Caso contrário, serão falsas com probabilidade de pelo menos 1/2 e b será um inteiro composto.

Quando b é ímpar, a ^ b, mdc (a,b) = 1, o símbolo de Jacobi tem valor em {-1,1} e pode ser eficientemente computado pelo algorítmo J(a,b): (Avaliação de (a/b)).

Algoritmo

```
if a = 1 then J := 1
else if a é par -> a = 0 (mod 2)
     then begin
          if (b² - l)/8 • 0 (mod 2)
             then J := J(a/2,b)
             else J := - J(a/2,b) end
     else if (a - l)*(b - l)/4 • 0 (mod 2)
          then J := J(b(mod a), a)
          else J := - J(b(mod a), a)
```

///

Para se proteger ainda mais contra os ataques, foram sugeridas algumas precauções na seleção de p e q

1. Os inteiros p e q devem diferir de alguns poucos dígitos no tamanho.

2. Ambos (p - 1) e (q - 1) devem possuir pelo menos um fator primo bastante grande.

3. O mdc (p-1, q-1) deve ser pequeno.

Para se atender a condição 2, gera-se primeiro um primo aleatório grande p' e então, gera-se p a partir de

$$p = i * p' + 1 \qquad \text{para} \quad i = 2, 4, 6 \ldots \qquad (4.8)$$

Outros métodos de se determinar números primos grandes existem, mas este método probabilístico foi apresentado no trabalho original sobre o RSA.

## 4.4 - UM ALGORÍTMO RÁPIDO DE DECIFRAGEM

0 fato de se utilizar no esquema do RSA, para garantir a segurança, exponenciação discreta módulo de um inteiro muito grande, produto de dois números primos grandes, resulta numa relativa complexidade de operações, em função do tempo. Isso quando comparado com sistemas convencionais, tais como o DES.

Quisquater e Couvreur propuseram um algoritmo para a decifragem do RSA que se baseia no teorema Chinês do Resto e em multiplicações modulares melhoradas [2]. Esse algoritmo, segundo os autores, chega a ser de 4 a 8 vezes mais rápido que os algoritmos

convencionais de decifragem do esquema RSA que se baseiam na utilização da expressão (4.2).

Antes da descrição do algoritmo, faz-se necessário elucidar as notações que serão utilizadas. Considere os resíduos das quantidades M (mensagem), C (criptograma) e d (chave de decifragem):

1. $C_1 \equiv C \pmod{p}$ e $C_2 \equiv C \pmod{q}$

2. $d \equiv d \pmod{p-1}$ e $d_2 \equiv d \pmod{q-1}$

3. $M_1 \equiv C_1^{d_1} \pmod{p}$ e $M_2 \equiv C_2^{d_2} \pmod{q}$

   ou

   $M'_1 \equiv M \pmod{p}$ e $M'_2 \equiv M \pmod{q}$

tendo-se sempre em vista a expressão (4.2).

Uma vez dados os inteiros p e q primos, onde $p < q$, considerar-se-á uma constante inteira A, tal que $0 < A < q - 1$ e que $Ap \equiv 1 \pmod{q}$. Esta constante é obtida aplicando-se o Algoritmo de Euclides para a determinação do mdc (p,q). Na determinação do mdc, desde que p e q são primos, tem-se

$$k_1 p + k_2 q = 1 \qquad (4.9)$$

onde as quantidades envolvidas, em termos de bits, são bem menores e a computação de **MJ** e **M^** pode ser feita em paralelo.

Outro ponto a ser observado é a escolha dos expoentes $d_1$ e $d_2$. Estes podem ser maiores que (p - 1) e (q - 1). Se o peso binário do expoente for menor que (p - 1) e (q - 1), a exponenciação modular será mais rápida.

Justamente porque no processo de decifragem o maior tempo consumido reside nas exponenciações modulares, será apresentado um algoritmo de exponenciação modular que determina P = (mod p) [2].

Na figura 4.1, encontra-se o diagrama funcional do processo de decifragem do RSA, onde se utiliza o algoritmo da exponenciação modular mencionado, bem como a computação em paralelo das quantidades **M'** e **M'**.

4.4.1 - Algoritmo da Exponenciação Modular

Inicialmente, faz-se algumas considerações, tais como, tomar o inteiro p como sendo maior que 1, com exatamente n bits, onde n = f 1°9₂ Pi * Supõe-se que um número qualquer d de n bits é representado como d = [d ... d d l .

PROCEDIMENTO DE EXPONENCIAÇÃO MODULAR (C,d,p)
{Dados os inteiros C, d, p, onde 0 ^ C < p, 0 ^ d < p - l , a rotina computa o inteiro P = $C^d$ (mod p), onde 0 ^ P < p }.

Inicialização: Q <— $2^n$ - p; P <— 1;

Passo 1: Para i = n - l , n - 2, 1

1.1 - Se $P_{n-1}$ = 1 , então P <— REDUCTION (P);

1.2 - P <— MODMUL (P,P,p,P);

1.3 - Se $d_4$ = 1, então P <— MODMULCO (P,p,table,P);

Passo 2: Se $P_{n-1}$ = 1 , então P REDUCTION (P);

Return P

PROCEDIMENTO REDUCTION (P);

{Dado o inteiro P de n bits, 0 í P < $2^n$, e o inteiro precomputado Q = $2^n$ - p (variável do tipo global), esta rotina retorna o valor P(mod p) entre 0 e p - 1}.

Inicialização: R <— P + Q;

Se $R_n$ = 1, então P <— [$R_{n-1}$ . . . $R_0$];

Return P

PROCEDIMENTO MODMUL (x,y,p,P);

{Dados os inteiros x, y e p, 0^ x < p, 0 ^ y < $2^n$, esta rotina computa o interio P = xy (modp). O inteiro P é um número de (n+1) bits, [P P . . . P P ] como saída, 0 ^ P < $2^n$ }.
n n - l l o

Inicialização: R <— Q + x; P <— 0;

Para i = n - l , n - 2 , 1

1. P <— P deslocado de um bit para esquerda;

2. Se *Y.—* 1# então

   Se $P_n$ = 1, então P <— [$P_{n-1}$ ... $P_0$ 1 + R

   senão P <— P + x;

3. Se $P_n$ = 1, então P <— [$P_{t}$ • • • $P_{0}$ ] + Q*

4. Se $P_n$ = 1, então P <— [$P_{n-1}$ ... $P_0$ + Q;

Return P

PROCEDIMENTO LOOK-UP TABLE (C,n,p,table);

{Dados os inteiros *C,* n e p, 0 ^ C < p, esta rotina computa a sequência *C,* 2C, $2^2$C, $2^{n-1}$C, cada valor sendo armazenado modulo p em uma tabela. Esta tabela é usada pela rotina MODMULCO }.

Inicialização: P <— C; table(0) <— C;

Para i = l , *2* , n - 1

1. P <— P deslocado de um bit para a esquerda;

2. Se $P_n$ = 1, então P <— [$P_{n-1}$ ... $P_0$ ] + Q;

3. Se $P_{n-1} = 1$, então P <— REDUCTION (P);

4. table(i) <— P;

Return

**PROCEDIMENTO MODMULCO** (x,p,table,P);

{Dados x, 0 s x < $2^n$, p e a tabela gerada pela rotina **LOOK-UP TABLE** para o inteiro C, esta rotina retorna o valor P = cx (mod p), 0 ≤ P < $2^n$ }.

Inicialização: P <— 0;

Para i = 1, 2, . . . , n - 1

Se $x_i$ = 1, então

1. P <— P + table(i);

2. Se P = 1, então P <— [P . . . P l + Q;

Return P.

2) Decifragem

2a) Pelo método convencional, utiliza-se a expressão (4.2) de forma que,

$$M = (C)^{d} \pmod{n}$$

$$M = (7)^{3} \pmod{15}$$

$$M = 3$$

2b) Pelo método do teorema Chinês do Resto, tem-se

$$C \equiv 7 \pmod{p} \quad \Rightarrow \quad C \equiv 7 \pmod{3}$$

$$C \equiv 1 \pmod{3}$$

$$C_2 = 7 \pmod{q} \quad \therefore \quad C_2 = 1 \pmod{5}$$

$$C_2 = 2 \pmod{5}$$

$$d \equiv 3 \pmod{p - 1} \qquad d \equiv 3 \pmod{2}$$

$$d_t = 1 \pmod{2}$$

$$d_2 = 3 \pmod{q - 1} \quad \Rightarrow \quad d_2 = 3 \pmod{4}$$

Donde então

# CAPITULO I

## INTRODUÇÃO

A Criptografia constitui-se em um dos ramos da Criptologia, que estuda os meios de como se manter secreta uma escrita, segundo a própria etmologia da palavra originária do Grego. Deseja-se com isso transformar uma informação sob a forma inteligível em uma forma não inteligível [1]. Ao processo de ocultação das informações ou dados costuma-se chamar de cifragem e ao processo inverso, chama-se decifragem. A maioria dos algoritmos utilizados nesses dois processos costuma utilizar um parâmetro K, mantido secreto, denominado chave.

De modo geral, em qualquer sistema de comunicação tem-se por princípio procurar manter restrita às partes envolvidas as informações que transitam por canais inseguros, isto é, canais sujeitos a interceptação por indivíduos não autorizados que poderão, por exemplo, modificar essas informações. Assim sendo, costuma-se utilizar técnicas de codificação e/ou cifragem para proteger as informações, sobretudo porque os meios atuais de comunicação são mais fáceis de serem interceptados.

Anteriormente, não havia importância em se determinar a diferença entre um código e uma cifra, pois tudo conduzia à idéia de proteção das informações. Porém, atualmente, a diferença tornou-se

1. $N_1 x_1 = 1 \pmod{p}$

$5x_1 \equiv 1 \pmod{3}$

$x_1 = 2$

2. $N_2 x_2 \equiv 1 \pmod{q}$

$3x_2 \equiv 1 \pmod{5}$

$\therefore \quad X_2 = 2$

Assim,

$$M = \sum_{i=1}^{2} N_i \times M_i' \pmod{n}$$

$$M = (N_1 \times M_1' + N_2 \times M_2') \pmod{15}$$

$$M = 28 \pmod{15} = 13$$

essa mensagem decifrada corresponde à mensagem enviada.

## 4.5 - CRIPTANÁLISE DO ALGORÍTMO RSA

O algoritmo RSA tem, até o momento, mostrado-se bastante seguro nas diversas aplicações. Rivest observou, entretanto, que

qualquer criptosistema para o qual exista uma prova construtiva da equivalência do esforço criptanalitico com a fatoração de inteiros, é vulnerável a ataques por texto cifrado escolhido [6], [7]«

Alguns pares de chaves do criptosistema RSA possuem certas propriedades que podem ser exploradas em vários ataques criptanalíticos. Alguns ataques utilizam-se da fragilidade existente no módulo n, através da descoberta de seus fatores primos p e q, outros, da fragilidade do expoente público e ou do expoente secreto d. O fato é que, muitas vezes, com o fim de se reduzir o tempo de execução dos processos de cifragem e decifragem do algoritmo, utiliza-se um expoente público, ou secreto, pequeno. Tendo por base esse fato, Michael Wiener, propôs um ataque criptanalítico a essa variação do RSA [8], onde fez uso de um algoritmo que se baseia em frações contínuas.

No ataque proposto por Wiener, o expoente público e o módulo n são usados para criar uma estimativa de uma fração que envolva o expoente secreto d. Para o caso em que e < n, mdc(p - 1, q - 1) for pequeno e p e q possuírem, aproximadamente, o mesmo número de bits, este ataque descobrirá expoentes secretos com até 1/4 de bits do módulo.

Existem meios de combate a esse ataque, por exemplo, se $^{e} > (PÇ)^{1'^{5}}$» ° algoritmo das frações contínuas não possui execução adequada garantida, quando se tem um expoente secreto de tamanho qualquer. Além disso, um outro fator que contribuiria para a inefi

ciência do método, seria fazer com que o mdc(p - 1, q - 1) fosse grande.

Esse ataque proposto por Wiener não se estende ao caso normal do RSA, onde o expoente secreto d possui, aproximadamente, o mesmo número de bits que o módulo n. Reafirma-se assim, que a tentativa de criptanálise do algoritmo RSA recai sempre na dificuldade de fatoração do módulo n.

Até a época do trabalho de Rivest, Shamir e Adleman [1], o algoritmo de fatoração mais rápido conhecido era o de Richard Shrorppel [5], que não fora publicado. Este algoritmo fatorava "n" em aproximadamente

$$\exp(\sqrt{\ln(n) * (\ln(\ln(n)))}) = n^{\sqrt{\ln(\ln(n))/\ln(n)}} \quad \bullet \quad (4.20)$$

passos. Com módulo de tamanho 200 dígitos, por exemplo, seriam necessários $1{,}2 \times 10^{23}$ operações e um tempo de $3{,}8 \times 10^{9}$ anos para se determinar os fatores primos de n, o que seria impraticável.

Hoje porém, tem-se conhecimento de vários métodos de fatoração de números compostos grandes. Mesmo assim, a complexidade ainda é alta, o que ainda permite que o algoritmo RSA seja preservado em

# REFERÊNCIAS BIBLIOGRÁFICAS

R. L. Rivest, A. Shamir e L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, vol. 21, n. 2, pp. 120-126, Fev. 1978.

J. J. Quisquater e C. Couvreur, "Fast Decipherment Algorithm for RSA Public-Key Cryptosystem", Electronics Letters, vol. 18, n. 21, pp. 905-907, Out. 1982.

Ernest. F. Brickell e Andrew M. Odlyzko, "Cryptanalysis: A Survey of Recent Results", Proceedings of the IEEE, vol. 76, n. 5, pp. 578-592, Maio 1988.

Gustavus J. Simmons, "How to Insure that Data Aqquired to Verify Treaty Compliance are Trustworthy", Proceedings of the IEEE, vol. 76, n. 5, pp. 621-627, Maio 1988.

Whitfiel Diffie, "The First Ten Years of Public-Key Cryptography", Proceedings of the IEEE, vol. 76, n. 5, pp. 560-577, Maio 1988.

Dorothy Elizabeth R. Denning, "Cryptography and Data Security", Addinson-Wesly, 1982.

James L. Massey, "An Introduction to Contemporary Cryptology", Proceedings of the IEEE, vol. 76, n. 5, pp. 533-549, Maio 1988.

Michael J. Wiener, " Cryptanalysis of Short RSA Secret Exponents ", IEEE Transaction on Information Theory, vol. 36, n. 3, pp. 553-558, Maio 1990.

# CAPÍTULO V

## APLICAÇÕES, CONCLUSÃO E SUGESTÕES

No decorrer do estudo realizado, viu-se que a exaltação provocada na imprensa popular e científica pelos sistemas criptográficos de chave pública por volta de 1976, levou ainda algum tempo para que esse tipo de criptosistema se estabelecesse. O entrave era ainda tanto, que mesmo nessa época de surgimento dos sistemas criptográficos de chave pública, o National Bureau of Standards dos Estados Uni, dos ainda lançou um sistema criptográfico convencional, o DES da IBM, que até hoje é utilizado e que tem se mostrado, até hoje, bastante eficiente, sobretudo, na transmissão de muitos dados, com velocidade invejável em relação aos criptosistemas de chave pública.

As implementações típicas de sistemas criptográficos de chave pública, tais como o RSA, operam a uma taxa de cerca de mil bits por segundo, enquanto a implementação mais rápida do DES, opera a uma taxa de milhões de bits por segundo [1]. Dessa forma, procura-se fazer uso dos sistemas criptográficos híbridos, onde os sistemas de chave pública são utilizados apenas em parte do processo, como, por exemplo, na distribuição de chaves para estabelecer as chaves compartilhadas no emprego dos sistemas convencionais.

As primeiras aplicações da criptografia de chave pública surgiram na Sandia após a publicação, em 1976, do artigo de Diffie e Hellman [2]. Com o posterior advento do RSA, a própria Sandia começou a desenvolver hardware capaz de conter as técnicas de cálculo empregadas nesse algoritmo, anunciando, em 1979, aplicativos na área de monitoramento sísmico. Rivest e outros pesquisadores do MIT também passaram a fazer implementações com o RSA. Passou-se a utilizar bastante o RSA, em quase muitas aplicações, devido a sua estrutura garantir, simultaneamente, privacidade e autenticidade.

Foi no início dos anos 80 que a tecnologia de chave pública transicionou da simples pesquisa pura para o desenvolvimento, a nível comercial, de produtos manufaturados. A Cylink Corporation, de Sunnyvale, Califórnia, foi a primeira, por exemplo, a produzir um chip, comercialmente disponível, contendo o RSA. Difundiu-se, assim, a preocupação com a segurança nas telecomunicações, nos sistemas de identificação de voz, no controle de acesso, enfim, começou a ser despertado o interesse dos próprios acadêmicos em explorar suas descobertas comercialmente.

Vê-se que um dos objetivos nas pesquisas dos sistemas criptográficos de chave pública tem sido demonstrar a equivalência entre muitos problemas, definidos como secundários, e os problemas de difícil solução que definem a força de um sistema [1].

Atualmente, a divulgação das aplicações vem tomando espaço

cada vez maior e vários padrões têm surgido a cada dia, sempre visando a utilização das técnicas de chave pública na distribuição de chaves e, principalmente, na geração de assinaturas digitais através de cartões inteligentes (smart cards).

Pode-se ainda verificar a utilização dos sistemas criptográficos de chave pública na correspondência eletrônica e no intercâmbio de dados,no controle de acesso e auditorias, como objeto de provas de falsificação, nos detetores de testes nucleares e, de modo geral, nos sistemas de reconhecimento, principalmente, com respeito à identificação de aeronaves.

Na seção que se segue, apresentamos algumas aplicações das técnicas criptográficas de chave pública difundidas hoje, não só nos setores militares ou diplomáticos, mas também na iniciativa privada.

## 5.1 - APLICAÇÕES DOS CRIPTOSISTEMAS DE CHAVE PÚBLICA

É do conhecimento da grande maioria que os algoritmos convencionais, tais como o DES, são largamente utilizados por serem mais rápidos. Contudo, o sigilo da chave secreta é um fator de fundamental importância nesses sistemas. É justamente nesse ponto, na distribuição dessas chaves, que atuam os sistemas criptográficos de cha

ve pública, por serem de mais baixo custo e mais seguros que os meios convencionais de se trocar a chave secreta, como por exemplo, postagem registrada, mensageiro confiável, etc.

Sabe-se que, em geral, as assinaturas convencionais são fáceis de serem falsificadas e difíceis de serem conferidas. Dessa forma, para minimizar os entraves burocráticos e garantir a segurança, passa-se a se utilizar assinaturas que tenham exatamente características opostas, ou seja, sejam de difícil falsificação e de fácil reconhecimento. Atualmente, já se usam as assinaturas digitais em ordens de compras, aplicações, contratos e mensagens eletrônicas de toda espécie. Uma assinatura digital consiste em um conjunto de símbolos que identifica uma pessoa, sendo função não só da mensagem que está sendo enviada com esta assinatura, como também da chave secreta que só o signatário possui. Assim, as técnicas de chave pública são as únicas conhecidas capazes de gerar assinaturas digitais com eficiência e privacidade, onde principalmente o algoritmo RSA se encontra em destaque.

Com as assinaturas digitais, já consideradas pela Eletronic Data Interchange (EDI), contratos e ordens de compra são assinados e entregues eletronicamente, por meio de mensagens cifradas, enviadas através de canais inseguros. Por exemplo, o Banco Britânico utiliza esse tipo de sistema de troca de dados, assim como tantos outros setores [3].

Um outro tipo de aplicativo importante, porque elucida mais ainda o uso de chaves públicas, é o controle de acesso. Este visa selecionar a entrada ou acesso a banco de dados em computadores, a redes de comunicação, à autorização de crédito, ou mesmo a locais físicos de extrema segurança. A identificação de um indivíduo pode basear-se no que ele possui, no que conhece ou em suas próprias características biométricas. Por exemplo, no acesso aos computadores a forma mais usual e convencional de acessar níveis é utilizar uma senha, mantida secreta pelo indivíduo e armazenada no próprio computador.

Em muitos sistemas de controle de acesso, dados pessoais de cada indivíduo são armazenados em um computador, que será consultado todas as vezes que alguém tentar acessar a rede de comunicação. Contudo, como hoje visa-se sempre rapidez na execução de um procedimento, para evitar a comunicação extra com o computador que contem a base de dados, o usuário utiliza um cartão com uma tarja magnética, ou uma chave de dados, ou um disco flexível, ou ainda um cartão inteligente que fornece todos os dados de identificação necessários [2]. Atualmente, tais cartões estão substituindo os cartões magnéticos convencionais. Eles apresentam o formato de um cartão de crédito normal, porém dispõem de um circuito integrado que não apenas contém células de memória para o armazenamento de grandes quantidades de dados pessoais, mas contém uma unidade central de processamento (CPU),

relevante. As informações são frequentemente codificadas e, posteriormente, cifradas tendo-se como objetivo maior segurança na sua transmissão.

Código vem a ser uma regra invariante para a substituição de parte de uma informação por outro objeto, não necessariamente da mesma espécie. Um código muito usado é o código ASCII, American Standard Code for Information Interchange, empregado em todos os computadores pessoais e terminais [2].

Cifra, assim como um código, também substitui parte de uma informação por outro objeto [2]. A diferença está no fato de que a substituição é feita segundo uma regra definida por uma chave secreta de conhecimento, apenas, do transmissor e do(s) legítimo(s) receptor(es), ou apenas de um deles, no caso dos sistemas não convencionais. No caso dos sistemas convencionais, supõe-se que ninguém, não autorizado, seja capaz de obter a informação ocultada, sem que tenha o conhecimento a priori da chave secreta.

Assim como os criptógrafos estão sempre desenvolvendo esforços para obter algoritmos cada vez mais eficientes, objetivando manter privacidade e autenticidade das informações, os chamados criptanalistas tentam não só obter o conteúdo das informações cifradas, mas, também, introduzir novas mensagens não autorizadas. Ao processo de se encontrar um método eficiente de decifragem do texto cifrado, sem o conhecimento da chave, chama-se Criptanálise, a qual constitui

memórias ROM, EPROM ou EEPROM e uma memória RAM.

A CPU existente nos smart cards não é suficiente para computar cálculos criptográficos envolvendo as funções de chave pública. Para tanto, costuma-se utilizar células especiais que realizam esses cálculos matemáticos, integradas ao chip. A Cylink tem sido a líder no desenvolvimento de chips de chave pública [3]. Na figura 5.1, tem-se uma idéia do chip baseado em tecnologia CMOS, contido no smart card da Cylink.

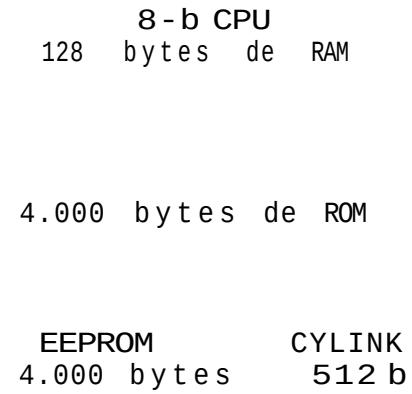



Fig. 5.1 - Chip CMOS da Cylink

que poderão ser constatadas através de auditorias.

Uma outra aplicação interessante inclue rádios digitais com leitoras de smart card que, acoplados aos automóveis, por exemplo, possibilitam o pagamento automático das taxas de pedágio ou de esta cionamento.

Com os smart cards, pode-se ainda, garantir a autenticidade e integridade de softwares regularmente executados, assim como de no vos programas e mesmo detectar a presença de vírus inclusos proposi tadamente por pessoas não autorizadas.

Um outro aplicativo da criptografia de chave pública é a utilização de sua estrutura como meio de objeto de prova de falsifi cação. Por exemplo, costuma-se medir, por um feixe de luz intenso que mede a intensidade da luz que atravessa o papel, a marca de im pressão do papel moeda, que é então digitalizada, cifrada por uma função de cifragem secreta criada pelo emissor do papel e registrada no próprio papel sob a forma digital, como acontece com o código de barra. Essa mesma idéia pode ser utilizada em todas as espécies de objetos, como acontece, por exemplo, na indústria automobilística, onde é feita uma pintura especial que funciona como assinatura digi t a l e que garante a originalidade da peça.

Hoje, com a tentativa de supremacia armamentista por muitos países também pode-se encontrar a atuação dos sistemas criptográfi cos. São empregadas assinaturas digitais para a verificação de possí

veis testes nucleares não autorizados. Por exemplo, duas potências militares acordam banir completamente de seus territórios os testes nucleares. Cada um dos dois países acordantes instalará sismográfos em várias localidades do território do país adversário. Esses sismo gráfos terão a função de detectar qualquer movimento do solo devido a uma explosão nuclear. Cada país pode suspeitar, que o adversário esteja, através dos instrumentos, enviando informações secretas re sultantes de espionagem. Dessa forma, faz-se necessário que os dados estejam disponíveis à apreciação pelos países envolvidos. Ao mesmo tempo, faz-se necessário saber que realmente se esteja, corretamen te, recebendo as informações, ou seja, deve-se ter certeza da auten ticidade e integridade das informações. Assim sendo, cada instrumen to deve conter um módulo para a criação de sua própria assinatura, que deve constar em cada bloco de dados sísmicos que grave. Esses da dos são transmitidos aos dois países, ficando eles impossibilitados de adulterarem o conteúdo dos instrumentos e provocarem, assim, um incidenteinternacional.

Por fim, tem-se outra aplicação dos sistemas criptográficos de chave pública nos sistemas de radar das aeronaves, que utilizam assinaturas digitais dispondo-a em qualquer sinal que receba. Nesse sistema o operador do radar cria um sinal de reconhecimento R e en via-o à aeronave. Por sua vez, a aeronave assina esse sinal e en via-o de volta para que se complete o reconhecimento por parte do

radar.

## 5.2 - RESULTADOS OBTIDOS

Com o trabalho realizado, conseguimos ampliar, substancialmente, a base de nossos conhecimentos na área de criptografia, sobretudo quanto aos criptosistemas de chave pública. Com isso, reunimos grande quantidade de material bibliográfico, o que nos possibilitou o desenvolvimento de uma abordagem teórica razoável.

Avaliamos, principalmente, as possibilidades de criptanálise dos algoritmos dos sistemas de chave pública, sobretudo, a criptanálise do algoritmo proposto por Merkle e Hellman, a Mochila com Alçapão. Entretanto, não chegamos à implementação do algoritmo de criptanálise, proposto por Shamir, por não dispormos do algoritmo chave por ele utilizado, o Algoritmo de Programação Inteira de Lenstra. De forma mais detalhada, contudo, constatamos a fragilidade hoje existente nesse algoritmo de Merkle e Hellman.

Ao mesmo tempo, dedicamos atenção a outro importante algorítmo de chave pública, segundo mostra o capítulo IV, o algoritmo RSA, onde tentamos destacar a sua criptanálise. Contudo, constatamos que este algoritmo ainda se mantém muito forte, uma vez que a tenta

III - Aprofundar os estudos quanto à utilização dos Smart Cards, tentando implementar protocolos e verificar os já existentes a respeito.

IV - Avaliar as variações do algoritmo RSA que se apoiam em estruturas matemáticas mais fortes, para obter maior velocidade no tempo de execução e maior dificuldade de criptanálise, sem contudo, comprometer os processos de cifragem e decifragem [5].

V - Ampliar a abordagem teórica e prática relativa ao criptosistema convencional mais amplamente utilizado, o DES, objetivando desenvolver (1) procedimentos eficientes de criptanálise para o sistema atual e (2) uma versão mais segura a partir de modificações do atual sistema.

VI - Investigar a concepção de se ter sistemas criptográficos, convencionais ou não, avaliando técnicas de assinaturas mais rápidos, bem como de autenticação, utilizando-se a teoria da Codificação de canal [6], [7], [8].

VII - Realizar um estudo detalhado das principais técnicas de fatoração e dos testes de primalidade existentes, visando o estabelecimento de procedimentos híbridos de desempenho superior.

VIII - Utilizar o algoritmo do Criptosistema RSA como teste de primalidade.

Dessa forma, cremos ter conseguido conquistar e aprimorar nossos conhecimentos, não só tendo proporcionado satisfação pessoal, mas sobretudo, contribuição para o encaminhamento das pesquisas na área.

# REFERÊNCIAS BIBLIOGRÁFICAS

[1] W. Diffie, "The First Ten Years of Public-Key Cryptography", Proceedings of IEEE, vol. 76, n. 5, pp. 560-577, Maio 1988.

[2] W. Diffie e M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, vol. IT-22, n. 6, pp. 644-654, Nov. 1976.

[3] J. K. Omura, "Novel Applications of Cryptography in Digital Communications", IEEE Communications Magazine, pp. 21-29, Maio 1990.

[4] H. P. Königs, "Cryptographic Identification Methods for Smart Cards in the Process of Standardization", IEEE Communication Magazine, pp. 42-48, Junho 1991.

[5] H. C. Williams,"A Modification of the RSA Public-Key Encryption Procedure", IEEE Transactions on Information Theory, vol IT-26, n. 6, pp. 726-729, Novembro 1980.

[6] T. R. N. Rao e K. H. Nam, " Private-Key Algebraic-Code Encryptions ", IEEE Transactions on Information Theory, vol. IT-35, n. 4, pp. 829-833, Julho 1989.

[7] Tatsuaki Okamoto,"A Fast Signature Scheme Based on Congruential Polynomial Operations", IEEE Transactions on Information Theory, vol. 36, n. 1, pp. 47-53, Janeiro 1990.

# APÊNDICES

# APÊNDICE I

## CLASSES DE COMPLEXIDADE

A teoria da complexidade classifica um determinado problema segundo o tempo ou espaço de memória mínimos necessários a sua solução tendo como base a máquina de Turing não determinística. Esta máquina, constitui-se em um modelo realístico, admitindo-se que os problemas que são solúveis de forma polinomial nesta, também o serão nos sistemas reais e vice-versa.

Definição A . I . l - MÁQUINA DE TURING DETERMINÍSTICA (DTM)

A máquina de Turing determinística com K trilhas, consiste em K trilhas semi-infinitas divididas em células que retêm um número finito de símbolos, varridas por um cabeçote que lê e escreve. Matematicamente, consiste em uma 7-upla definida por

$$DTM = (Q,T,I,\hat{o},b,q_o\ q_f)$$

onde

1. Q representa o conjunto de estados.
2. T representa o conjunto de símbolos de uma trilha.
3. I representa o conjunto de símbolos de entrada; I £ T.

b £ T-I, representa o símbolo blank.

$q_0$ corresponde ao estado inicial.

$q_f$ corresponde ao estado final ou aceito

ô corresponde à função do próximo movimento que mapeia um sub conjunto $Q \times T^k$ em $Q \times (T \times \{L,R,S\})^k$. Ou seja, para alguma (k+l)-upla consistindo de um estado e k símbolos, fornece um novo estado e k pares, cada par consistindo de novos símbolos e uma direção de movimentação para o cabeçote da trilha.

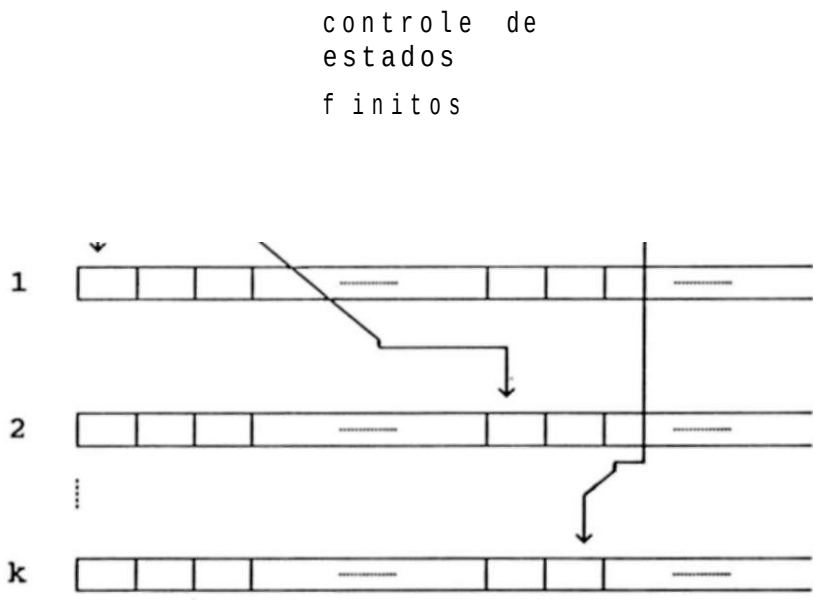



Fig. A.I.l - Máquina de Turing Determinística

o outro ramo da Criptologia [1].

Em 1949, Shannon introduziu com seu trabalho [3] a fundamentação teórica à Criptografia, tendo por base um outro trabalho seu, publicado em 1948 [4], onde estabeleceu os princípios fundamentais da teoria da Informação. O que Shannon fez foi medir a segurança teórica de uma cifra a partir da incerteza existente sobre a informação não cifrada, dado que se tenha recebido uma informação cifrada, estabelecendo, assim, as noções de sigilo perfeito e de segurança computacional de uma cifra [cap. II].

## 1.1 - NOÇÕES DE TEORIA DA INFORMAÇÃO

A teoria da Informação está vinculada a dois problemas fundamentais: o problema da codificação da fonte de informação e o problema do canal ruidoso.

O problema do canal ruidoso é análogo ao problema do sigilo considerado nos sistemas criptográficos [5]. Transmite-se uma mensagem M através de um canal inseguro, ou seja, com ruido, para um receptor, conforme a figura 1.1.

Na figura A.I.l, tem-se uma máquina DTM com múltiplas trilhas. A operação da máquina é determinada por um programa primitivo chamado de controle finito.

De acordo com o estado do controle finito e dos símbolos que estão sob varredura, a DTM pode executar uma ou todas as seguintes operações:

1. Trocar o estado do controle finito.
2. Gravar novos símbolos sobre os símbolos atuais da trilha em qualquer das células que esteja sendo varrida.
3. Mover qualquer dos cabeçotes das trilhas independentemente, uma célula a direita (R), uma a esquerda (L) ou mantê-los estacionários (S).

Definição A.1.2 - MÁQUINA DE TURING NÁO-DETERMINÍSTICA (NDTM)

Uma NDTM com k trilhas consiste em uma 7-upla

$$(Q, T, I, ô, b, q_0, q_f)$$

onde todos os componentes têm os mesmos significados que na DTM, exceto pela função ô que mapeia $Q \times T^k$ em subconjuntos de $Q \times (T \times \{L, R, S\})^k$. Dado um estado e uma lista de k símbolos, a função Ô leva a um conjunto finito de escolhas de próximas mudanças; onde ca

da escolha corresponde a um novo estado com k símbolos e k ações de movimentação para o cabeçote, não podendo haver escolha de um novo estado a partir de outro.

Definição A.1.3 - FUNÇÕES POLINOMIALMENTE LIMITADAS

Se $f, g_1, g_2, \ldots, g_m$ são funções de valores reais, então f é dita ser polinomialmente limitada por $g_1, g_2, \ldots, g_m$ se existe uma função **0,** tal que $<p \leq f$ e que **0** surja de uma sequência de composições, a partir das funções $g_1, g_2, \ldots, g_m$ e a partir de alguns polinómios.

Definição A.1.4 - ALGORÍTMO DE TEMPO POLINOMIAL

Um algoritmo é chamado de polinomial ou de tempo polinomial se sua função do tempo de execução for uma função polinomialmente limitada.

Definição A.1.5 - PROBLEMAS TRATÁVEIS

Os problemas solúveis em tempo polinomial são também chamados de tratáveis, caso contrário de intratáveis (hard).

Na figura A.1.2 vê-se várias classes importantes de complexidade e algumas de suas possíveis relações.

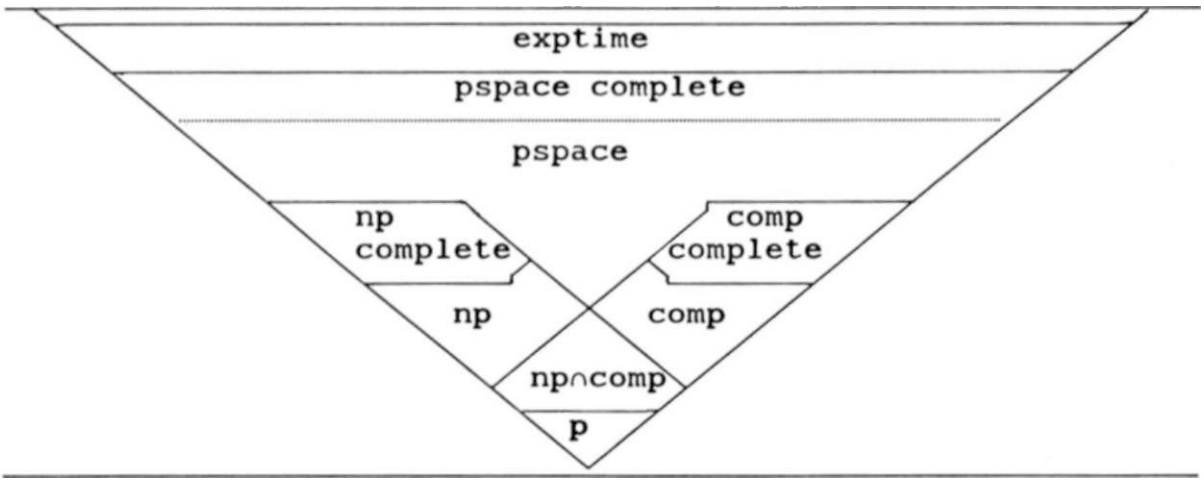



Fig. A.1.2 - Classes de Complexidade

Para maiores esclarecimentos quanto às classes de complexidade vide referência [1].

Definição A.1.6 - CLASSE *P*

Define-se a classe *P-time* como o conjunto de todos os problemas aceitos por uma máquina DTM cuja complexidade de tempo de solução seja polinomial. A partir do conjunto L de linguagens existentes, tomando-se o conjunto L(M) das linguagens aceitas por uma máquina DTM, define-se a classe P como,

*P-time* = { L / existe uma máquina M e um polinómio p(n), tal que essa máquina seja de complexidade de tempo polinomial p(n) e L(M) = L } [2]

Definição A.1.7 - CLASSE *NP*

Define-se como *NP* ao conjunto de todos os problemas aceitos por uma máquina DTM cuja complexidade de tempo de solução seja polinomial.

As definições (A.1.6) e (A.1.7) podem ser feitas em função de qualquer modelo de máquina e não apenas em termos das máquinas de Turing. Por outro lado, sabe-se que a classe *NP* inclui a classe P, pois qualquer problema solúvel polinomialmente na máquina DTM também o é em uma máquina NDTM [1]. Não se prova, porém, que a classe P não

ou se qualquer um desses problemas pertencer à classe *P*, então *PSpace = P.*

Definição A.1.12 - CLASSE *EXPTIME*

Consiste dos problenas que são solúveis em tempo exponen ciai e incluem os problemas *PSpace.*

Viu-se que o problema da mochila estudado classifica-se como um problema WP-complete.

# APÊNDICE II

# PROGRAMAÇÃO MATEMÁTICA E APROXIMAÇÃO DIOFÁNTICA

## 1. PROGRAMAÇÃO MATEMÁTICA

O estudo de programação matemática tem por objetivo os problemas de otimização onde se tenta maximizar ou minimizar uma quantidade específica que dependa de um número finito de variáveis de entrada. A essa quantidade denomina-se objetivo. As variáveis de entrada podem estar relacionadas por uma ou mais condições (restrições) ou serem totalmente independentes. Para maior compreensão, tem-se algumas definições e as referências [ 3 ] , [ 4 ] .

Definição A.II.l - PROGRAMAÇÃO MATEMÁTICA

Programação matemática constitui-se em uma ferramenta que lida com problemas de otimização, sujeitos a restrições, onde o objetivo é expresso como uma função matemática e as restrições expressas pelo conjunto de relações { =, s , > }. Ou seja,

$$\text{objetivo} : z = f(x_1, x_2, \ldots, x_n)$$

restrições : $g_1(x_1, x_2, \ldots, x_j)$

$g_2(x_1, x_2, \ldots, x_n)$

\

$g_m(x_1, x_2, \ldots, x_n)$

Definição A.II.2 - PROGRAMAÇÃO LINEAR

Um problema de programação matemática é dito ser linear se a função que define o objetivo $f(x_1, x_2, \ldots, x_n)$ e todas as funções que definem as restrições $g(x_1, x_2, \ldots, x_n)$, para $1 \leq i \leq m$, forem todas funções lineares de seus argumentos. Ou seja,

$$f(x_1, x_2, \ldots, x_n) = c_1 x_1 + c_2 x_2 + \ldots + c_n x_n$$

e

$$g(x_1, x_2, \ldots, x_n) = a_{11} x_1 + a_{12} x_2 + \ldots + a_{1n} x_n$$

onde Cj e $a_{ij}$, para $1 \leq i \leq m$ e $1 \leq j \leq n$, são constantes conhecidas.

Definição A.II.3 - PROGRAMAÇÃO INTEIRA

Trata-se de um problema de programação linear onde se tem a restrição adicional de que as variáveis de entrada *x^, x^, . .., x^* são números inteiros.

## 2. ALGORÍTMO DE LENSTRA

Em 1983, Lenstra mostrou que para um dado número natural n, existe um algoritmo polinomial capaz de solucionar os problemas de programação linear inteira com n variáveis. Trata-se de um algoritmo que soluciona um sistema de desigualdades lineares de n variáveis inteiras [4].

Teorema A.II.l

Existe um algoritmo polinomial que determina, para qualquer sistema Ax ^ b de desigualdades racionais lineares, ura vetor y de inteiros que satisfaz à desigualdade Ay ^ b, ou um vetor inteiro c não nulo tal que,

(max{cx I Ax **Í** b} - rain{cx | Ax * b}) * 2n(n + 1) $2^{n(n \text{ " } 1)/4}$

onde n corresponde ao número de colunas da matriz A.

Corolário A.II.l - ALGORÍTMO DE LENSTRA

Para cada número natural n, existe um algoritmo polinomial que determina uma solução inteira para um dado sistema racional Ax s b, com n variáveis, ou que decide se existe ou não solução para o sistema.

## 3. APROXIMAÇÃO DIOFÃNTICA

Aproximação Diofântica diz respeito ao problema de se aproximar números reais por números racionais de denominador inferior, podendo ser realizada através do método das frações contínuas [4], [5].

Teorema A.II.2 - TEOREMA DE DIRICHLET

Sejam a um número real e c um número positivo tal que 0 < e 3 1. Então existem inteiros p e q, tal que

onde 11.11 representa a norma Euclidiana ( $\|x\| = \sqrt{x^T x}$ ).

De modo geral, pode-se afirmar que Aproximação Diofântica Simultânea consiste no estudo da aproximação de um vetor de números reais $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ por um vetor de números racionais $(p_1/q, p_2/q, \ldots, p_n/q)$ onde todos os elementos desse vetor possuem o mesmo denominador [6].

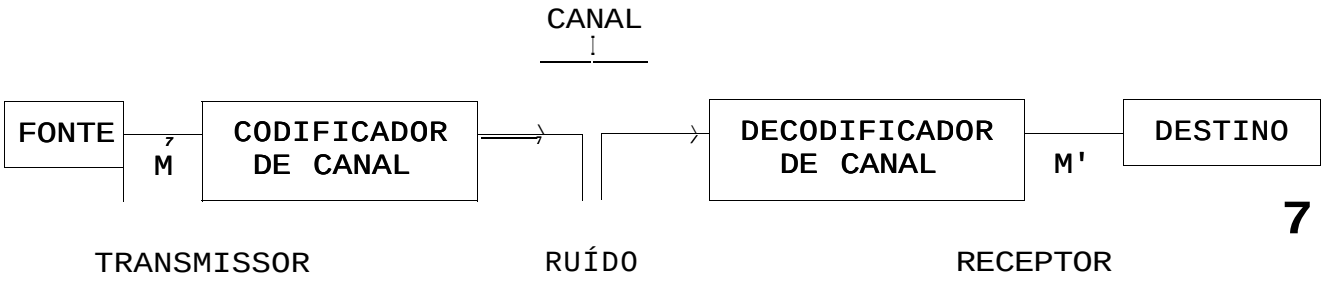



Fig. 1.1 - Comunicação por Canal Inseguro

Se uma mensagem distorcida M' for recebida, deseja-se que o receptor seja capaz de recuperar a mensagem originalmente enviada. Para tornar isso possível, o emissor acrescenta à M, bits redundantes, de forma que os erros ocorridos na transmissão possam ser corrigidos ou pelo menos detectados, o que determinaria um pedido de retransmissão da informação [ 5 ] .

Nesse contexto, o papel do criptanalista é similar ao do receptor no problema anterior, enquanto que o papel do transmissor é um pouco diferente, porque este tem por objetivo tornar impraticável a descoberta da mensagem por pessoa não autorizada.

Segundo Shannon, a quantidade de informação contida em uma mensagem, I(M), é medida pela incerteza associada à mensagem. Especi

.

APÊNDICE III

## NOÇÕES BÁSICAS DE TEORIA DOS NÚMEROS

Neste apêndice apresenta-se alguns resultados da Teoria dos Números, fundamentais ao estudo dos sistemas criptográficos, sobretudo aos de chave pública [1], [7], [8].

### Definição A.III.1 - NÚMERO PRIMO

Um inteiro $p > 1$ é dito ser um número primo se possuir como únicos divisores os inteiros positivos 1 e p. Todo e qualquer número inteiro, maior que 1, que não seja um número primo é denominado de número composto.

### Teorema A.III.1 - TEOREMA FUNDAMENTAL DA ARITMÉTICA

Todo inteiro positivo $n > 1$, pode ser expresso como um produto de potências de primos, de forma única,

$$n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$$

onde, para $i = 1, 2, \ldots, r$, $p_i$ é um primo com $p_1 < p_2 < \ldots < p_r$ e $k_i$, etc.

é um inteiro positivo.

Teorema A.III.2 - TEOREMA CHINÊS DO RESTO

Sejam n , , .../ n^ inteiros positivos, tais que mâcfxij,]! ) = 1 para i *j . Então, o sistema de congruências lineares

$$x \bullet a_i \pmod{\ }$$

$$x \bullet a_2 \pmod{n_2}$$

$$x = a^ \pmod{n^}$$

tem solução simultânea única, modulo $n_1 n_2 \ldots n_r$ .

Prova

Consideremos o produto n = n n....n e, para cada k = 1, 2,...r, seja N^ o produto de todos os inteiros onde se omite o fator n^, ou seja,

$$N_k = \frac{n}{n} = n_1 \ldots n_{k-1} n_{k+1} \ldots n_r$$

Por hipótese, os são relativamente primos, portanto,

$mdc(N_k, n_k) = 1$. Assim, é possível se determinar uma solução única x^ para a congruência N^x = 1 (mod n j .

Quer-se provar que o inteiro

$$x = a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_r N_r x_r$$

é uma solução simultânea para o sistema de congruências.

Pelo fato de que 0 (mod nj , para i*k, tem-se que

$$x = a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_r N_r x_r = a_k N_k x_k \cdot k' \pmod{n,}$$

Como o inteiro x^ foi escolhido de modo a satisfazer N^x • 1 (mod $n_{re}$), força-se

$$x = a_k .1 = a_k \pmod{n_k}$$

Assim, mostra-se que existe uma solução para o sistema de congruências. Para mostrar que essa solução é única, suponha que exista uma outra solução x' que satisfaça às congruências. Então,

x • a^ • x' (mod nj para k = 1,2, r

o que implica que $n_k$ (x - x') para cada valor de k. Com mdc($n_1$,n ) = 1. tem-se que $n_1 n_2 ... n_r$ l(x - x'), portanto, n|(x - x') e, assim, x • x' (mod n) e a solução é única.

///

Teorema A.III.3 - TEOREMA DE FERMAT

Se p é um primo, então

$$M^{p-1} = 1 \pmod p$$

para todo M e p primos entre si, e

$$M^p = M \pmod p$$

para todo M.

Prova

Como o mdc(M,p) = 1, então, p / M; portanto, considere os (p - 1) múltiplos positivos inteiros de M,

$$M, 2M, 3M, ..., (p - 1)M$$

Nenhum desses números é congruente módulo p com qualquer outro. Se isso acontecesse, então

$$rM \bullet sM \pmod{p} \qquad i < r < s \text{ í } (p - 1)$$

e M poderia ser cancelado restando $r \bullet s \pmod{p}$, o que é impossí vel. Portanto, os inteiros múltiplos de M devem ser congruentes módu lo p a 1, 2, 3, ..., (p - 1) em alguma ordem. Assim, multiplicando essas congruências, tem-se

$$M.2M.3M. \ldots (p - 1)M = 1.2.3. \ldots (p - 1) \pmod{p}$$

donde

$$M^{p-1}(p - 1)! = (p - 1)i \pmod{p}$$

desde que $p / (p - 1)!$, então

$$M^{p-1} = 1 \pmod{p}$$

e como p / M, então, pode-se multiplicar essa congruência por M o que conduz a

$$M^{p} = M \pmod{p}$$

///

Definição A.III.2 - FUNÇÃO DE EULER $\varphi(.)$

Para todo $n \geq 1$, a função $\varphi(n)$ representa o número de inteiros positivos que não excedem n e que são relativamente primos a n.

Teorema A.III.4

Se $n = p^k$ onde p é um número primo e $k > 0$, então

$$\theta(n) = \theta(p^k) = p^k - p^{k-1} = P^{k-1}(l - P)$$

Prova

Sabe-se que $mdc(n,p^k) = 1$ se só se $p \nmid n$, assim existem $p^{k-1}$ inteiros entre 1 e $p^k$, divisíveis por p, ou seja,

$$p,\ 2p,\ 3p,\ \ldots\ (p^{k-1})p$$

Como o conjunto de inteiros de 1 até $p^k$ possui $p^k$ elementos, o conjunto $\{l, 2, \ldots, p^k\}$ possui exatamente $(p^k - p^{k-1})$ inteiros que são relativamente primos a $p^k$. Portanto, pela definição (A.III.2), tem-se

$$\theta(n) = \varphi(p^k) = p^k - p^{k-1}$$

///

O teorema (A.III.4) pode ser generalizado para $n = p_1^{k} p_2^{k} \ldots p_r^{k}$, lembrando-se que a função $\theta(n)$ é uma função multiplicativa, ou seja, se mdc(m,n) = 1, então

$$\theta(n.m) = \theta(n)\theta(m)$$

Teorema A.III.5

Se o inteiro $n > 1$ tem a fatoração em primos dada por $n = p_1^{k} p_2^{k} \ldots p_r^{k}$, então,

$$\theta(n) = (p_1^{k} - p_1^{k-1})(p_2^{k} - p_2^{k-1}) \ldots (p_r^{k} - p_r^{k-1})$$

Teorema A.III.6 - TEOREMA DE EULER

Se n e M são inteiros positivos onde mdc(M,n) = 1, então,

$$M^{\theta(n)} = 1 \pmod{n}$$

Prova

Sejam $a_1, a_2, \ldots a_{\theta(n)}$ inteiros positivos menores que n,

Vê-se assim que o teorema de Euler é uma generalização do teorema de Fermat.

Definição A.III.3 - SÍMBOLO DE JACOBI [8]

Este símbolo é denotado por J(a,n) e definido por

$$J(a,n) = \begin{cases} 1 & \text{se } a = 1 \\ J(a/2,n)(-1)^{(n^2-1)/8} & \text{se } a \text{ é par} \\ J(n(\text{mod } a),n)(-1)^{(a-1)(n-1)/4} & \text{se } a > 1 \text{ for ímpar} \end{cases}$$

onde mdc(a,n) = 1.

Definição A.III.4 - PSEUDO-PRIMO DE FERMAT

Um número composto N para o qual

$$a^{N-1} = 1 \pmod N$$

é chamado pseudo-primo para a base a.

Definição A.III.5 - PSEUDO-PRIMO FORTE

Um número N composto ímpar com $(N - 1) = d.2^s$, onde d é

ímpar, é dito ser um pseudo-primo forte para a base a, se

$$a^{d} = 1 \pmod{N}$$

ou

$$a^{d \cdot 2^{r}} = 1 \pmod{N}$$

para $r = 0, 1, 2, \ldots, s - 1$.

dos e raramente falharem. A falha, nesse caso, encontra-se relacionada com a indicação errônea de que um número composto é primo [9]. Alguns métodos encontram-se relacionados a seguir.

Testes de Primalidade
- -> Método de Fermât
- -> Método de Euler
- -> Método dos Pseudo-Primos Fortes
- -> Método de Lehmer
- -» Método de Lucas
- -> Método de Pocklington
- -» Método de Lenstra

Dentre esses métodos enfocaremos o de Fermat e o dos Pseudo Primos Fortes, cujas aplicações já são relativamente suficientes para a determinação de números primos; os demais encontram-se detalhados na referência [10].

De forma geral, se na aplicação dos testes de primalidade as condições para a existência dessa não forem satisfeitas, pode-se garantir que o número N é composto; entretanto, nada pode ser afirmado caso as condições sejam satisfeitas.

## 1.1 - MÉTODO DE FERMAT

O Teorema de Fermat [A.III] pode ser aplicado como teste para

ficamente, Shannon definiu

$$I(M) = \log_2(1/P(M)) \quad \text{bits}$$

Para uma fonte de informação, esta quantidade é medida por uma função de distribuição de probabilidade sob o conjunto de todas as possíveis mensagens.

Definição 1.1 - ENTROPIA

Sejam , $X_2, \ldots, X^{\wedge}$ n possíveis mensagens de uma fonte X, com probabilidades $p(X_1)$, $p(X_2), \ldots, p(X_n)$, respectivamente, onde $\sum_{i=1}^{n} P(X_i) = 1$. Define-se a entropia de X pela média ponderada

$$H(X) = -\sum_{i=1} p(X_i) \log p(X_i) \quad \text{bits/símbolo}$$

ou, em termos da quantidade de informação,

$$H(X) = \sum_{X} p(X)\, I(X)$$

Quando se mede a entropia de um conjunto de mensagens, mede

ra a determinação de números compostos, tratando-se de um poderoso teste para se mostrar a não primalidade de um dado número.

Existem condições em que a aplicação do teste de Fermât falha, identificando um número N composto como sendo primo. Esses números são classificados como Pseudo-Primos de Fermât [A.III].

Definição A.IV.l - TESTE DE FERMAT

Se mdc(a,N) = 1 e $a^{N-1} \equiv 1 \pmod{N}$, então pode-se afirmar que N é um número composto, sendo sempre possível encontrar uma base a menor que N.

Como exemplo de falha do teste de Fermât, consideremos N = 341 = 11*31 e a = 2, onde,

$$a^{N-1} \equiv 1 \pmod{341} \qquad (1.2)$$

Contudo, ao considerarmos a = 3, constata-se que N é um número composto, pois,

$$3^{340} \equiv 56 \pmod{341} \qquad (1.3)$$

A partir do conhecimento de todos os números pseudoprimos, o uso do teorema de Fermât constitui-se num rápido teste de primalidade, principalmente para números de um dado tamanho [9]. D. H. Lehner preparou uma tabela com todos os pseudoprimos de Fermât abaixo de $2 \times 10^{9}$ na base 2, com nenhum fator menor que 317, que começava em $10^{7}$. Carl Pomerance, John Selfridge e Samuel Wagstalf mostraram que abaixo de $25 \times IO^{9}$ existem 1770 pseudoprimos simultaneamente para as bases 2, 3, 5 e 7. Cada teste de Fermât é executado em no máximo $2.1og_{2}N$ passos.

1.1.1 - Algoritmo de Fermât

O algoritmo usado para computar a^(mod N), baseia-se na representação binária do expoente d, onde

$$d = /3_{0} + \mathbf{0}\ 2 + \ldots + /3_{g}2^{8} \qquad (1.4)$$

e os **0^** são dígitos binários de $d = 2$, de forma que se possa determinar

$$a^{d} = a^{i=o^{1}}$$

$$a = n^{a} \qquad (1.5)$$

Antes de se computar a expressão (1.5), precisa-se determinar os dígitos binários do expoente d, e para isso existem algorítmos prontos. Apresentamos um procedimento para a obtenção dos dígitos menos significativos do expoente.

Procedimento

P I . Se d f o r ímpar, então /3$_q$= 1. Caso contrário, *fi*$_Q$= 0.

P2. Faça d • (d - 0 )+ 2.

///

Os demais dígitos do expoente d podem ser obtidos da mesma forma. Assim sendo, para se obter a^(mod N), faz-se

Procedimento

P I . (Inicialização) L e r a, d e N.

Fazer Prod := 1 e a2j = a.

P2. Enquanto d > 0 faça

2a. Se d for ímpar, então, prod := prod * a2j (mod N).

2b. Faça d := d DIV 2 ; a2j := $(a2j)^2$ (mod N)

///

Este programa opera apenas se $N^2$ for menor que o maior inteiro que puder ser armazenado no computador, sendo importante utilizar a aritmética de múltipla precisão. O número de multiplicações e reduções (mod N) envolvidas se encontra entre $[\log_2 d]$ e $2.[\log_2 d]$, dependendo do número de dígitos l's que há em N.

Além dos Pseudoprimos, existe uma outra espécie de números compostos conhecidos como números de Carmichael [9] que não são revelados pelo método de Fermat, a menos que a base a seja um divisor de N, o que fere a condição de que mdc(a,N) = 1. Como exemplo desse tipo de número, tem-se N = 561 = 311 * 17.

## 1.2 - MÉTODO DOS PSEUDO-PRIMOS FORTES

Neste teste, onde se procura determinar se um número N é composto ou primo, faz-se uso do critério de Euler [9] em lugar do

critério de Fermat, bem como do conceito de pseudoprimos fortes [A.III].

. . . 9

Inicialmente, como exemplo de pseudoprimos abaixo de 25*10 para as bases 2, 3 e 5, simultaneamente, tem-se 13 números que aparecem listados na tabela (IV.1).

| Números | Fatoração |
|---|---|
| 25326001 | 2251.11251 |
| 1 61304001 | 7333.21997 |
| 9 60946321 | 11717.82013 |
| 11 57839381 | 24061.48121 |
| 32 15031751 | 151.751.28351 |
| 36 97278427 | 30403.121609 |
| 57 64643587 | 37963.151849 |
| 67 70862367 | 41143.164569 |
| 143 86156093 | 397.4357.8317 |
| 155 79919981 | 88261.176521 |
| 184 59366157 | 67933.271729 |
| 198 87974881 | 81421.244261 |
| 212 76028621 | 103141.206281 |

Tab. IV.1 - Pseudoprimos Fortes para as bases 2, 3 e 5.

Utilizando-se a tabela (IV.1), passa-se à determinação da

primalidade ou não de N através de um procedimento simples, como se segue.

Procedimento

P1. Verifica-se se N é um pseudo-primo na base 2. Caso contrário, N é composto.

P2. Verifica-se se N é um pseudo-primo na base 3. Caso contrário, N é composto.

P3. Verifica-se se N é um pseudo-primo na base 5. Caso contrário, N é composto.

P4. Se N for um dos treze números constantes da tabela (IV.1), então N é composto, caso contrário N é primo.

///

Observa-se que se N for um número primo serão necessários três passos, caso contrário no passo 1, como mais frequentemente acontece, será revelada a não primalidade de N. Este teste de prima

lidade é mais forte que o teste de Euler. Na referência [9], pp. 100-101, encontramos um simples programa, em PASCAL, para teste de primalidade de qualquer número ímpar abaixo de $25*10^9$.

## 2 - MÉTODOS DE FATORAÇAO

O estudo da decomposição de inteiros compostos grandes em seus fatores primos, avançou consideravelmente nesses últimos anos, principalmente, com o advento dos computadores de alta velocidade. Dessa forma, não se pode fornecer uma boa classificação dos métodos de fatoração em utilização, uma vez que os estudos nesse campo são frequentes e contínuos. Apresentamos alguns principais métodos de fatoração para os quais é sempre prudente verificar antes, se realmente o número em questão é composto. Assim mesmo, a escolha entre os vários métodos disponíveis não é fácil. Por exemplo, há certos metodos que são desvantajosos caso o número a ser fatorado possua uma forma matemática em particular.

A seguir apresentamos uma classificação geral de alguns métodos de fatoração de números compostos, dos quais apenas três são abordados neste apêndice. Os demais encontram-se disponíveis na referência [9].

Métodos de Fatoração

-> Método das Divisões
-> Método de Fermat
-> Método de Euler
-> Método de Gauss
-» Método de Legendre
-» Métodos de Pollard
-» Método (p+1)
-» Método de Shank
-> Método das Frações Contínuas
-» Método dos Crivos
-> Método dos Crivos Quadráticos
-» Método de Schroeppel
-> Método de Schnorr-Lenstra
-> Método de Monte Carlo

## 2.1 - MÉTODO DE FERMAT

Este método de fatoração de números inteiros é um dos mais antigos, porém não é um dos mais eficientes [2]. A idéia é tentar escrever o inteiro N = a.b como uma diferença de dois números, ou seja, $N = x^2 - y^2 = (x - y).(x + y)$, onde x deve ser maior que $\sqrt{N}$.

Dessa forma, faz-se $m = \lfloor \sqrt{N} \rfloor + 1$ como sendo o menor valor possível de x. Verifica-se, então, se $z = m^2 - N$ corresponde a um quadrado; em caso afirmativo, $N = x^2 - y^2$ e conclui-se a fatoração. Caso contrário, faz-se $m = m + 1$ e computa-se, novamente, $(m + 1)^2 - N = z + 2m + 1$. Como exemplo considere N = 13199, onde $\sqrt{N} = 114{,}88...$; então, m = 115 e z = 26; n as operações de busca por um quadrado, chega-se à tabela:

| m | 2m + 1 | z |
|---|---|---|
| 115 | 231 | 26 |
| 116 | 233 | 257 |
| 117 | 235 | 490 |
| 118 | 237 | 725 |
| 119 | 239 | 962 |
| 120 | 241 | 1201 |
| 121 | 243 | 1442 |
| 122 | 245 | 1685 |
| 123 | 247 | 1930 |

| m | 2m + 1 | z |
|---|---|---|
| 124 | 249 | 2177 |
| 125 | 251 | 2426 |
| 126 | 253 | 2677 |
| 127 | 255 | 2930 |
| 128 | 257 | 3185 |
| 129 | 259 | 3442 |
| 130 | 261 | 3701 |
| 131 | 263 | 3962 |
| 132 | 265 | 4225 |

Os números z são calculados adicionando-se sempre 2m + 1 Para m = 132, chega-se a $z = 4225 = 65^2$. Assim,

$$N = 132^2 - 65^2$$
$$= (132 - 65).(132 + 65) = 67.197$$

A principal dificuldade com este método é a quantidade de passos necessários à fatoração. De modo geral, para N = a.b, produto de dois primos, com a < b, a fatoração será alcançada quando m = (a + b)/2, sendo pequena a quantidade de trabalho necessário para isso. Para o fator a = kv' N , 0 < k < 1, o número de ciclos necessários a obtenção da fatoração é $\left( \frac{(1 - k)^2}{2k} \right) \sqrt{N}$, sendo da ordem 0(/~N~~) . O método só é considerado praticável para fatores próximos de *V* N . Po de-se considerar um algoritmo cujo loop principal é muito rápido em computadores, mas que é inconveniente quando executado manualmente. Parte-se do princípio de que dado um número ímpar N, seja-se capaz de determinar o maior fator de N que seja menor ou igual a *V* N . Pa

ra isso tem-se o seguinte procedimento:

Procedimento

PI. (Inicialização) Faça x' <— 2[ / N J + 1, y' <— 1,
r L /~N~J²- N

P2. (Teste de r) Se r **Í** 0, vá para o passo 4.

P3. (Passo y) Faça r <— r - y', y' <— y' + 2 e retorne ao passo 2.

se a sua incerteza com relação ao número de bits de informação que deve ser conhecido para especificá-lo.

No estudo sobre a segurança de uma cifra, Shannon definiu grandezas que se relacionam com a incerteza das mensagens, bem como grandezas que medem a capacidade teórica de que o criptanalista venha a quebrar uma dada cifra.

Definição 1.2 - AMBIGÜIDADE

Dada uma mensagem Y no conjunto $Y_1, Y_2, \ldots, Y_m$, onde $\sum_{i=1}^{n} P(Y_i) = 1$ / $P_y(x) = P(X|Y)$ é a probabilidade condicional da mensagem X dada a mensagem Y e P(X,Y) é a probabilidade conjunta das mensagens X e Y, define-se ambigüidade como sendo a entropia de X dada Y, isto é,

$$H_y(X) = \sum_{X,Y} P(X,Y) \log (1/P(X))$$

No contexto da Criptologia, a ambigüidade $H_c(K)$ mede a incerteza que tem o criptanalista sobre a chave K, dado que tenha examinado a mensagem cifrada C [5]. Quando H (K) vai a zero significa

Procedimento

PI. Gerar uma lista com todos os primos e potências de primos até um certo limite G, por exemplo G = 100.000. Escrever, para cada quadrado, cubo, etc... de um primo, o correspondente primo em lugar da potência prima em questão.

P2. Escolher um valor a, por exemplo a = 13, e computar

$$b_i \equiv b_{i-1}^{p_i} \pmod{N} \qquad (2.1)$$

onde $p_i$ representa o i-ésimo inteiro da lista de primos. A sequência (2.1) deve ser iniciada com $b_1 = a$.

P3. Computar o produto acumulado

$$Q_n = \prod_{i=1}^{n} (b_i - 1)$$

e testar periodicamente o $mdc(Q_n, N)$, a fim de verificar se um fator p de N surgiu.

///

Para se verificar em quanto tempo este algoritmo determina um fator de N, suponha que

$$N = \prod_{i} P_i^{\alpha_i} \qquad (2\text{-}3)$$

e

$$p_i - 1 = \prod_{j} 3_j^{\beta_j}$$

e considere que $q_i$ seja a maior potência prima na fatoração de $p_i - 1$. Assim sendo, o fator $p_t$ será obtido assim que se exceda o valor $q_i$ na lista de potências primas utilizadas. Significando, portanto, que o fator $p_t$ de N, para o qual o valor q é o menor de todos os fatores p de N, aparece primeiro e, assim, fatores primos grandes podem ser rapidamente detectados por esse método.

No trabalho de H. C. Williams [12], tem-se um exemplo para o qual os fatores p e q de $(10^{95} + 1)$ e $(3^{136} + 1)$, respectivamente, onde

$$p = 121450506296081$$

$$q = 2670091735108484737$$

são mencionados como sendo determinados através do método (p-1) de Pollard. Tem-se ainda nesse exemplo, que os fatores de (p-1) e (q-1) são

$$p - 1 = 2^4 * 5 * 13 * 19^2 * 15773 * 20509$$

$$q - 1 = 2^7 * 3^2 * 7^2 * 17^2 * 19 * 569 * 631 * 23993$$

## 2.3 - MÉTODO p DE POLLARD

Este método tem por base uma idéia estatística, o método de Monte Carlo [10], [13], introduzida por Pollard e refinada por Richard Bret [14]. Consiste em,

P I . Construir uma sequência de inteiros { x ^ que é periódica (mod p)

P2 . Procurar um período, ou seja, encontrar i e j , tais que,

$$x = x \pmod{p}$$

P3. Identificar o fator p de N.

///

Analisando-se as exigências requeridas, tem-se que a primeira é muito fácil de ser cumprida. Para tanto, considere uma sequência do tipo

$$x_i = F(x_{i-1}, x_{i-2}, \ldots, x_{i-s}) \pmod m$$

onde s é uma constante independente de i e F é um polinómio. Considere $x_1, x_2, \ldots, x_s$ como valores iniciais de dados. Como todos os $x_k$'s são dados (mod m), existem apenas m diferentes valores para cada $x_k$ e $m^s$ sequências distintas $x_{i-1}, x_{i-2}, \ldots, x_{i-s}$ de s números consecutivos $x^{\wedge}$. Desta forma, após $m^s + 1$ passos, ocorrerão duas sequências idênticas, $x_{i-1}, x_{i-2}, \ldots, x_{i-s}$ e $x_{j-1}, x_{j-2}, \ldots, x_{j-s}$. Pela definição, cada $x_k$ depende dos s valores precedentes e assim, se as duas sequências são idênticas para k distintos, então $x_{i-k}$ e $x_{j-k}$ devem ser os mesmos, significando que a sequência $x^{\wedge}\}$ é periódica, exceto no começo onde pode ser aperiódica. Considere como exemplo a sequência de Fibonacci (mod 11), definida por

$$x_i = x_{i-1} + x_{i-2} \pmod{11}$$

com $x_1 = x_2 = 1$.

Assim, consegue-se a seguinte sequência,

1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 11, 2, 3 ... (mod 11)

Após 10 elementos a sequência se repetirá.

Com a segunda exigência, se o período em que a sequência se repete for curto, basta se fazer uma análise comparativa; contudo, o mesmo não se pode fazer se o período for longo e, neste caso, tem-se um caminho a seguir. Suponha que a sequência {X } (mod m) possua uma parte não periódica de tamanho a e um período 1. O período é determinado pelo algoritmo de Floyd, onde se pergunta se $*_{21} - *_{t}$ (mod m) [9].

Com a terceira exigência, utiliza-se, como no método (p-1), o algoritmo de Euclides para determinar o mdc($x_{21} \sim x$^ (mod N),N) = d. Em geral d = 1, mas quando $*_{21} = x_{t}$ (mod p), d será divisível por p.

Em síntese, requer-se que a sequência {X } seja fácil de ser calculada, que o período seja pequeno e que o uso do algoritmo de Euclides não acarrete muito tempo de computação.

Pollard determinou que em uma sequência $\{x_{i}\}$ (mod p) de inteiros aleatórios, um elemento é repetitivo após aproximadamente cv/p~ passos. Mas em lugar disso, pode-se utilizar uma sequência de inteiros pseudo-aleatórios. A escolha recairá em se determinar $x_{i+1} = ax_{j}$ (mod p) para um dado valor fixo de a; mesmo assim, isso não produzirá números suficientemente aleatórios { x ^ para um pequeno período de apenas cv/p passos. Na busca pelo fator p, deve-se acumular o produto

$$Q = \prod_{J=i} (*_{21} - x_{i}) \mod N$$

e aplicar-se o algoritmo de Euclides apenas quando i for um múltiplo de 100. Na referência [9], tem-se um pequeno programa em PASCAL e um exemplo elucidativo.

# REFERÊNCIAS BIBLIOGRÁFICAS

[1] D. E. R. Denning, "Cryptography and Data Security", Addison Wesley, 1982.

[2] A. V. Aho, J. E. Hopcroft e J. D. Ullman, "The Design and Analysis of Computer Algorithms", Addison-Wesley, 1974.

[3] R. Bronson, "Pesquisa Operacional", McGraw Hill, 1985.

[4] A. Schrijver, "Theory of Linear and Integer Programming", John Wiley & Sons Ltd., Amsterdam, 1986.

[5] Ivan Niven, "Diophantine Approximations", John Wiley & Sons, 1963.

[6] E. F. Brickell e A. M. Odlyzko, "Cryptanalysis: A Survey of Recent Results", Proceedings of the IEEE, vol. 76, n. 5, Maio 1988.

[7] D. M. Burton, "Elementary Number Theory", Allyn and Bacon, 1976.

[8] Alan G. Konheim, "Cryptography: A Primer", John Willey & Sons, New York, NY, 1981.

[9] Hans Riesel, "Prime Numbers and Computer Methods for Factoti. zation", Birkhauser, 1985.

[10] Donald E. Knuth, "The Art of Computer Programming : Seminumeri cal Algorithms", vol.2, 2d. ed., Addison-Wesley Publishing Company, USA 1981.

[11] J. M. Pollard, "Theorems on Factorization and Primality Testing", Proceedings Cambr. Philos. Soc, vol 76, pp. 521-528, 1974.

[12] H. C. Williams, "A (p+1) Method of Factoring", Math. Comp., vol. 39, pp. 225-234, 1982.

[13] J. M. Pollard, "A Monte Carlo Method for Factorization", Nordisk Tidskrift för Informationsbehandling (BIT), vol. 15, pp. 331-334, 1975.

[14] Richard P. Brent, "An Improved Monte Carlo Factorization Algorithm", Nordisk Tidskrift för Informationsbehandling (BIT), vol. 20, pp. 176-184, 1980.

que não existe incerteza e a cifra é teoricamente quebrável. Assim, Shannon precisou definir a distância de unicidade de uma cifra.

Definição 1.3 - DISTÂNCIA DE UNICIDADE

Trata-se do menor comprimento N de texto cifrado, tal que H (K) se aproxime de 0, ou seja, define-se como a quantidade de texto cifrado necessário para se determinar de maneira única a chave K.

Supondo-se que as mensagens cifradas e não cifradas originam-se de um alfabeto finito de L símbolos, e considerando que em toda linguagem existe uma taxa absoluta $R = \log_2 L$, definida como o número máximo de bits de informação que podem ser codificados em cada caracter, e supondo ainda que todas as sequências de mensagens são equiprováveis, define-se a redundância de uma linguagem como sendo $D = R - r$, onde $r = H(X)/N$ é a taxa da linguagem e N corresponde ao comprimento da mensagem. Desta forma, existe um total de $2^{RN}$ mensagens de comprimento N, das quais $2^{rN}$ são mensagens com sentido e $(2^{RN} - 2^{rN})$ são mensagens sem sentido. Supondo na criptanálise que cada mensagem seja igualmente provável, tem-se que a probabilidade de se obter uma mensagem com sentido e, consequentemente, uma solução errada é dada por

$$II(K) - DN = rN * 0$$

sendo a cifra teoricamente inquebrável.

Dessa forma, observou-se que a compressão dos dados seria uma ferramenta extremamente útil [6], eliminando a redundância da linguagem e dificultando a criptanálise.

Com o crescimento observado nos anos 60 nas comunicações e com a disseminação de recursos computacionais é que o reconhecimento da necessidade de proteção dos sistemas ficou definitivamente estabelecido. Os algoritmos criptográficos passaram a ter como base problemas matemáticos ou estatísticos.

A abordagem na área de Criptografia tendo por base a Teoria da Informação foi deixada a parte. Só por volta de 1989 [7], retomou-se os estudos relativos à segurança teórico-prática dos sistemas criptográficos, tendo por base esta Teoria. Assim, hoje, a Teoria da Informação não pode ser vista como irrelevante à Criptografia, e sim como uma ferramenta fundamental ao seu desenvolvimento [6], [7], [8].

## 1.2 - CHAVES PÚBLICAS

Nos sistemas convencionais o que é mais preocupante é o si

gilo da chave de cifragem/decifragem, assim como o meio de distribuição dessa chave. Para se ter uma idéia, para que um dos 1.000 usuários de um sistema deseje se comunicar com os demais, seria necessário produzir 999 cópias da chave e ter o extremo cuidado de mantê-las em completo sigilo. Entretanto, o mesmo não acontece nos chamados sistemas de chave pública. Os principais problemas que levaram a sua concepção foram:

1. O problema da distribuição de chaves. Se duas pessoas que não se conhecem desejarem manter uma comunicação sigilosa através dos meios criptográficos convencionais, precisam de uma chave do conhecimento apenas dos dois e de mais ninguém.

2. O problema da autenticidade das informações. Supondo que um indivíduo A envie uma mensagem para um indivíduo B, este precisa de um procedimento que lhe permita assegurar a autenticidade da mensagem, isto é, se realmente foi A quem de fato a enviou.

Os sistemas criptográficos de chave pública apontaram na *áireção* de uma abordagem mais teórica que permite o desenvolvimento de protocolos criptográficos com demonstradas características de segurança [9].

conceitos empregados em criptografia.

No capítulo III, tem-se o estudo detalhado do algoritmo da Mochila com Alçapão, onde são descritas suas principais características, variações e, principalmente, a criptanálise desse algoritmo.

O capítulo IV é dedicado ao estudo, do algoritmo RSA, sendo elucidado seu princípio de funcionamento e as tentativas de criptanálise mais recentes.

O capítulo V trata das principais aplicações da criptografia, em especial a de chave pública, nos meios atuais de comunicação, o estado em que se encontram as pesquisas na área, de algumas sugestões e do resultado obtido com esse estudo; o de reunir todo um arcabouço teórico da área com o fim de impulsionar pesquisas futuras.

Finalmente, tem-se os apêndices I, II, III e IV que agrupam assuntos correlatos e de apoio ao material apresentado nos capítulos mencionados.

# REFERÊNCIAS BIBLIOGRÁFICAS

[1] M. E. Smid e D. K. Branstad, "The Data Encryption Standard : Past and Future", Proceedings of the IEEE, vol. 76, n. 5, pp. 550-558, Maio 1988.

[2] G. J. Simmons, "Cryptology", Enciclopédia Britânica, vol. 16, pp. 913-924B, 1986.

[3] C. E. Shannon, "Communication Theory of Secrecy Systems", Bell Syst. Tech. J., vol. 28, pp. 656-715, Out. 1949.

[4] C. E. Shannon, **"A** Mathematical Theory of Communication", Bell Syst. Tech. J., vol. 27, pp. 379-423, Julho e pp. 623-656, Out. 1948.

[5] D. E. R. Denning, "Cryptography and Data Security", Addison Wesley, 1982.

[6] J. L. Massey, "An Introduction to Contemporary Cryptology", Proceedings of the IEEE, vol. 76, n. 5, pp. 533-549, Maio 1988.

[7] James L. Massey, "The Relevance of Information Theory to Modern Cryptography", Proceedings of the 1990 Bilkent International Conference on New Trends in Communication, Control and Signal Processing (BILCON'90), Julho 1990, Ankara, Turquia.

[8] U. M. Maurer, **"A** Provably-Secure Strongly-Randomized Cipher", Outubro 1989, Monte Veità, Ascona, Suiça.

[9] W. Diffie, "The First Ten Years of Public-Key Cryptography", Proceedings of the IEEE, vol. 76, n. 5, pp. 560-577, Maio 1988.

[10] E. F. Brickell e A. M. Odlyzko, "Cryptanalysis : A Survey of Recent Results", Proceedings of IEEE, vol. 76, n. 5, pp. 578-592, Maio 1988.

CAPÍTULO **II**

## NOÇÕES DE CRIPTOLOGIA

A Criptologia continua sendo uma forte área de pesquisa que se tornou de interesse geral, constando em muitas publicações, principalmente após o avanço da tecnologia dos sistemas digitais.

A palavra criptologia origina-se do grego, onde CRIPTO significa SIGILO e LOGIA significa PALAVRA. Portanto, trata-se da ciência utilizada para descrever todo o campo das comunicações que devem ser mantidas em sigilo. Como vimos no capítulo I , a Criptologia envolve a Criptografia e a Criptanálise.

A Criptografia consiste no estudo de princípios e técnicas através das quais a informação pode ser ocultada por meio de cifras, que nada mais são que meios de codificação das mensagens, ou seja, métodos secretos de escrita. Essas cifras mais tarde serão reveladas por seu legítimo receptor através do correto emprego de uma chave secreta, devendo ser impossível ou computacionalmente impraticável, a uma pessoa não autorizada, descobrir a informação enviada.

A Criptanálise consiste no estudo de princípios e técnicas através das quais se recuperam as informações secretas, a partir das cifras, sem o conhecimento da chave que possibilite naturalmente a

obtenção dessa informação.

## 2.1 - CONSIDERAÇÕES GERAIS

De um modo geral, um criptógrafo busca estudar sistemas matemáticos que assegurem o sigilo (privacidade) e/ou a autenticidade de mensagens quando transmitidas através de um canal de comunicação inseguro. Enquanto isso, o criptanalista busca desfazer o trabalho do criptógrafo, pela quebra das cifras utilizadas ou pelo simples forjamento de sinais cifrados que poderão ser aceitos como autênticos.

Um sistema criptográfico é uma família única $\{S^\}/$ de transformações inversíveis, tal que um espaço { M } de mensagens claras ou textos originais, seja mapeado num espaço { C } de mensagens cifradas, mais frequentemente conhecidas como criptogramas. Ou seja,

$$S_R : \{ M \} \longrightarrow \{ C \}$$

O parâmetro k que seleciona a transformação S é chamado de chave, sendo selecionado a partir de um conjunto finito { K } que corresponde ao espaço de chaves.

Ao processo de transformação do texto claro em texto cifra

mo a fatoração de números inteiros compostos grandes ou a extração de logaritmos discretos em um corpo finito GF(q), onde q foi cuidadosamente escolhido, possa ser resolvido com comparável esforço. Um exemplo desse tipo seria o criptosistema RSA, que será abordado com com maiores detalhes no capítulo IV.

Nesses dois casos acima citados, a segurança depende apenas da dificuldade computacional de se solucionar um problema difícil. Por isso, pode-se simplesmente tratar-se esses dois tipos de sistema como computacionalmente seguros. Enquanto isso, todo sistema que resista a qualquer ataque criptanalítico, independentemente dos recursos computacionais e do tempo que um oponente levaria para desçobrir a mensagem, é dito ser incondicionalmente seguro. A busca de códigos inquebráveis tem se constituído em um dos temas mais antigos na pesquisa criptográfica.

A segurança incondicional resulta da existência de múltipias soluções, com sentido, para um mesmo criptograma. Um exemplo desse tipo de criptosistema é aquele dito ser "one time pad", ou seja, aquele que é utilizado apenas uma única vez. Esse tipo de sistema é inquebrável [4]. O texto pleno é combinado com uma chave de mesmo tamanho, escolhida aleatoriamente, que só será utilizada uma única vez. Esse tipo de sistema pode ser impraticável para muitas aplicações devido à quantidade de chaves que deveriam ser geradas ao mesmo tempo e ao tamanho de cada chave.

Por outro lado, um criptosistema computacionalmente seguro contém informação suficiente para se determinar de maneira única o texto pleno e a chave. A segurança, nesse caso, está no custo computacional devido à dificuldade que deve encontrar o criptanalista em obter o texto pleno sem o conhecimento a *priori* da chave. Esse problema recai no domínio da complexidade computacional e análise de *algorítmos* [4].

Os sistemas criptográficos foram divididos em duas categorias ou classes extensas: sistemas de cifragem bit a bit e sistemas de cifragem de bloco.

Definição 2.1 - SISTEMAS DE CIFRAGEM BIT A BIT

Os sistemas de cifragem bit a bit (stream ciphers) processam o texto claro caracter a caracter, produzindo uma sequência de bits pseudo-aleatória que é adicionada módulo 2 aos bits do texto pleno. A mensagem M é segmentada em sucessivos caracteres $m_1, m_2, \ldots$, cifrando-se cada $m_i$ com o i-ésimo elemento $k_i$ de uma chave $K = (k_1, k_2, \ldots, k_i, \ldots)$, isto é,

$$E_K(M) = E_{k_1}(m_1)\, E_{k_2}(m_2) \ldots$$

Definição 2.2 - SISTEMAS DE CIFRAGEM DE BLOCO

Os sistemas de cifragem de bloco (block ciphers) atuam em grandes blocos do texto pleno de forma que uma mudança pequena na entrada de um bloco produza uma mudança maior na saída resultante [1]. Neste caso, a mensagem é segmentada em blocos sucessivos $M_t$, M , cifrando-se cada M^ com a mesma chave K, isto é,

$$E_K(M) = E_K(M_1)\, E_K(M_2) \ldots$$

A propagação de erro existe nas cifras de bloco, enquanto na cifragem bit a bit não há propagação, pois cada caracter do texto cifrado é independentemente cifrado e decifrado. Códigos corretores de erro são normalmente aplicados após a cifragem com o fim de proteger as informações [5].

Na seção 2.2, a seguir, teremos um relato histórico sobre a evolução da Criptologia.

## 2.2 - RELATO HISTÓRICO

A história de que se tem conhecimento a respeito dos códigos e cifras é bastante extensa e interessante, datando de aproxima

damente 4.000 anos atrás, no tempo da grande civilização Egípcia. É provável que a arte de se procurar esconder o verdadeiro sentido das comunicações escritas date de épocas ainda mais remotas. Muitas e várias foram as técnicas empregadas ao longo dos séculos. Sempre os códigos secretos tiveram posição de destaque em algumas técnicas criptográficas.

A época pré-científica da criptologia remota desde a Antiguidade, com os gregos, até 1949, sendo até então praticada mais como uma arte do que mesmo como uma ciência.

Julius Cesar escrevia a Cícero e a outros amigos na época da Roma Antiga, a aproximadamente 2.000 anos atrás, empregando técnicas de cifragem extremamente simples para a época atual. Uma cifra criptográfica recebeu, em sua homenagem, o seu nome, cifra de Cesar. Nessa cifra cada letra do texto claro original é substituída pela terceira letra subsequente a esta, no alfabeto Latim. Isso é feito ciclicamente para todas as letras do alfabeto. Na seção 2.3, veremos que esta cifra é classificada como de substituição simples, utilizada nos sistemas criptográficos convencionais, sendo portanto de fácil quebra.

Em 1794, em Nova York, foi gravada uma inscrição cifrada numa tumba nos fundos da igreja de Trinity, onde não se utilizou um alfabeto convencional [5]. Uma cifra similar também foi encontrada em uma tumba na igreja de St. Paul, em Nova York, em 1796. Apenas 100

anos depois apareceu a primeira solução publicada para as cifras.

Por vários séculos criptanalistas tentaram solucionar uma cifra que apontava para um tesouro enterrado na Virgínia, por volta de 1820, deixada por Thomas Jefferson Beale. Esta cifra foi a primeira das três cifras deixadas por Beale. A segunda cifra foi solucionada por James Ward nos idos dos anos 1880. A terceira cifra ainda não conseguiu ser decifrada. Muitos continuaram tentando decifrar as cifras de Beale e encontrar o propenso tesouro.

O desenvolvimento das cifras polialfabéticas, ou seja, onde se tem múltiplas substituições, começou em 1568 com uma publicação de Leon Battista Alberti, onde era definida uma cifra que consistia em um disco no qual se faziam várias substituições que podiam ser mudadas durante o processo de cifragem.

Ainda por volta do século 16, atribuiu-se a um criptologista francês, Blaise de Vigenère, uma cifra que se baseia na substituição dos caracteres de um alfabeto por outros do alfabeto deslocado.

A cifra conhecida como de Playfair, assim denominada em homenagem ao cientista inglês Lyon Playfair, tendo sido inventada em 1854 por um amigo deste, Charles Wheatstone, e utilizada pelos ingleses durante a primeira Guerra Mundial, corresponde a uma cifra de substituição poligrâmica [5],

Em 1917, Gilbert Vernam, funcionário da American Telephone and Telegraph Company, projetou um dispositivo criptográfico para

as comunicações telefônicas baseadas no código Baudot de 32 caracteres. Cada caracter é representado como uma combinação de 5 marcas e espaços, correspondentes aos bits 1 e 0, respectivamente, nos computadores digitais. Esta cifra é similar à cifra de Vigenère. A grande idéia de Vernam foi a introdução de uma chave que pudesse ser utilizada apenas uma vez (one time pad). Cada bit da chave que é usado para cifrar um bit de mensagem, é escolhido aleatoriamente, aumentando se assim a segurança contra ataques criptanalíticos.

Durante a segunda Guerra Mundial, surgiram as máquinas a rotor que definem cifras de substituição polialfabéticas que consistem em um banco de t rotores ou discos, ligados por um fio. A máquina Enigma, por exemplo, inventada por Arthur Scherbius e utilizada pelos alemães, utilizava um odômetro a rotor [5].

Foi justamente por volta da Segunda Guerra Mundial que a comunidade científica reconheceu que os matemáticos poderiam prestar contribuições à criptologia. Então, em 1949, com a publicação do trabalho de Shannon, "Communication Theory of Secrecy Systems", introduziu-se a era científica da criptologia de chave secreta. Shannon estabeleceu limites na quantidade de chaves secretas que devem ser transferidas seguramente ao receptor legítimo.

Em 1976, a criptografia clássica ou convencional de até então, tomou novo direcionamento com a publicação do trabalho de Diffie e Hellman [4]. Determinava-se assim o início da era dos siste

mas criptográficos de chave pública, o que levou à divisão da criptografia em duas fases bem distintas: Clássica ou Convencional e Moderna ou de Chave Pública. Estas duas fases serão melhor avaliadas nas seções 2.4 e 2.5.

Daí em diante, o desenvolvimento mais importante veio a ocorrer em 1977, quando o National Bureau of Standards (NBS) anunciou o Data Encryption Standard (DES), a ser utilizado em aplicações do governo dos Estados Unidos não classificadas. O DES é uma técnica de criptografia convencional que cifra blocos de dados de 64 bits com uma chave de cifragem de 56 bits. Discutia-se se o comprimento da chave de cifragem seria ou não suficiente. Contudo até hoje o DES continua sendo utilizado, principalmente em transações on-line no setor comercial privado e industrial, onde a cada 5 anos o governo revisa seu nível de segurança [6].

Em 1978, Pohlig e Hellman publicaram um esquema de cifragem que se baseia na computação de exponenciais em um corpo finito [7]. Nesta mesma época, Rivest, Shamir e Adleman também publicaram um esquema similar que ficou conhecido no mundo científico como RSA [8], o qual se constitui num dos objetos de nosso estudo. O algoritmo RSA é descrito em detalhes no capítulo IV.

Ainda em 1978, Merkle e Hellman propuseram um esquema de cifragem cuja segurança dependia da dificuldade de se solucionar o problema clássico da mochila, mostrando como converter uma mochila

simples em uma mochila com alçapão, até então mais difícil de ser solucionada sem alguma informação adicional. O algoritmo da mochila é introduzido no capítulo III, onde são encontrados maiores detalhes a respeito.

Neste mesmo ano de 1978, Robert McEliece apresentou um criptosistema de chave pública [9], tendo como base códigos corretores de erros.

A partir de então, grande foi a corrida dos pesquisadores para a busca de sistemas criptográficos mais poderosos, no sentido de oferecer maior segurança na privacidade e autencidade das comunicações. Começou, então, a surgir a figura mais ativa do criptanalista. Vários sistemas, bem como variações dos mesmos já amplamente aceitas pela comunidade internacional, passaram a ser atacados, na tentativa de serem criptanalizados. Em 1984, Adi Shamir apresenta um algoritmo de criptanálise, em tempo polinomial, do criptosistema de Merkle-Hellman com apenas uma iteração [10]. Este algoritmo é descrito no capítulo III. Neste mesmo ano, Ernie Brickell anuncia a quebra desse mesmo algoritmo de Merkle-Hellman, com até 40 iterações, utilizando um CRAY-1 [11].

Em virtude da eficiência dos sistemas criptográficos de chave pública, em especial o RSA, as aplicações encaminharam-se para a solução de antigos problemas encontrados nos sistemas criptográficos convencionais, como por exemplo, a distribuição das chaves de cifra

gem e decifragem, o gerenciamento dessas chaves, a correspondência eletrônica, a troca de dados, etc. Ainda com o objetivo de preservar a autenticidade das comunicações, sobretudo nas transações comerciais e de credenciamento ou controle de acesso, cresceu a utilização das assinaturas digitais e dos cartões de identificação [8], [12], [13]. Atualmente, pesquisas são feitas na utilização dos mesmos princípios criptográficos de chave pública em cartões inteligentes que conseguem armazenar maiores informações e fornecer maior segurança [14].

## 2.3 - SIGILO PERFEITO

Em todo sistema criptográfico, visa-se manter o sigilo da informação, através da manutenção do sigilo de uma chave. Shannon considerou a segurança sob duas formas, introduzindo as noções de segurança teórica e segurança prática.

Com a noção de sigilo ou segurança teórica, onde se leva em consideração que as condições para a criptanálise são ilimitadas, Shannon chegou à condição de que a quantidade de chaves secretas necessarias à construção de uma cifra teoricamente segura, era extremamente grande em certas aplicações. Assim sendo, Shannon buscou o si

gilo prático, onde admitiu que as condições para a criptanálise são limitadas. Essa segurança prática é a que se pretende obter com os sistemas de chave pública, por exemplo. Massey afirmou, em recente trabalho [15], que, atualmente, a única porta aberta ao estudo da segurança prática, desde o trabalho de Shannon, é a nova abordagem relativa a Teoria da Informação, desenvolvida por Maurer.

Shannon, no estudo sobre a segurança teórica, fez duas suposições fundamentais. A primeira dessas suposições é que a chave secreta de cifragem seria utilizada apenas uma única vez. A segunda suposição é que o criptanalista só teria acesso aos criptogramas, ficando limitado, portanto, a apenas um tipo de ataque criptanalítico. Assim, Shannon passou a definir o que seria sigilo perfeito e a avaliar as propriedades das informações em sistemas criptográficos, levando em consideração três classes de elementos :

1. As mensagens $M_1, M_2, \ldots, M_n$, em texto claro, que são finitas em número e podem ocorrer com probabilidades a priori

$$P(M_1),\ P(M_2),\ \ldots,\ P(M_n)$$

onde $\sum_{i} P(M_i) = 1$, $1 \leq i \leq n$ ;

2. As mensagens $C_1, C_2, \ldots, C_n$, em texto cifrado, podem ocor

rer com probabilidades

$$P(C_1), P(C_2), \ldots, P(C_m)$$

onde $\sum_{i} P(C_i) = 1$, $1 \leq i \leq m$;

3. As chaves K que são escolhidas com probabilidades a priori P(K), onde $\sum P(K) = 1$

Assim sendo, Shannon definiu que o sigilo é perfeito se a interceptação de C não fornecer nenhuma informação adicional ao criptanalista sobre M. Ou seja, as probabilidades a posteriori são iguais às probabilidades a priori, independentemente desses valores [2]. Formalmente,

$$P_c(M) = P(M) \qquad (2.1)$$

Uma condição necessária e suficiente para se ter sigilo perfeito é obtida a partir do teorema de Bayes aplicado a expressão (2.1), isto é

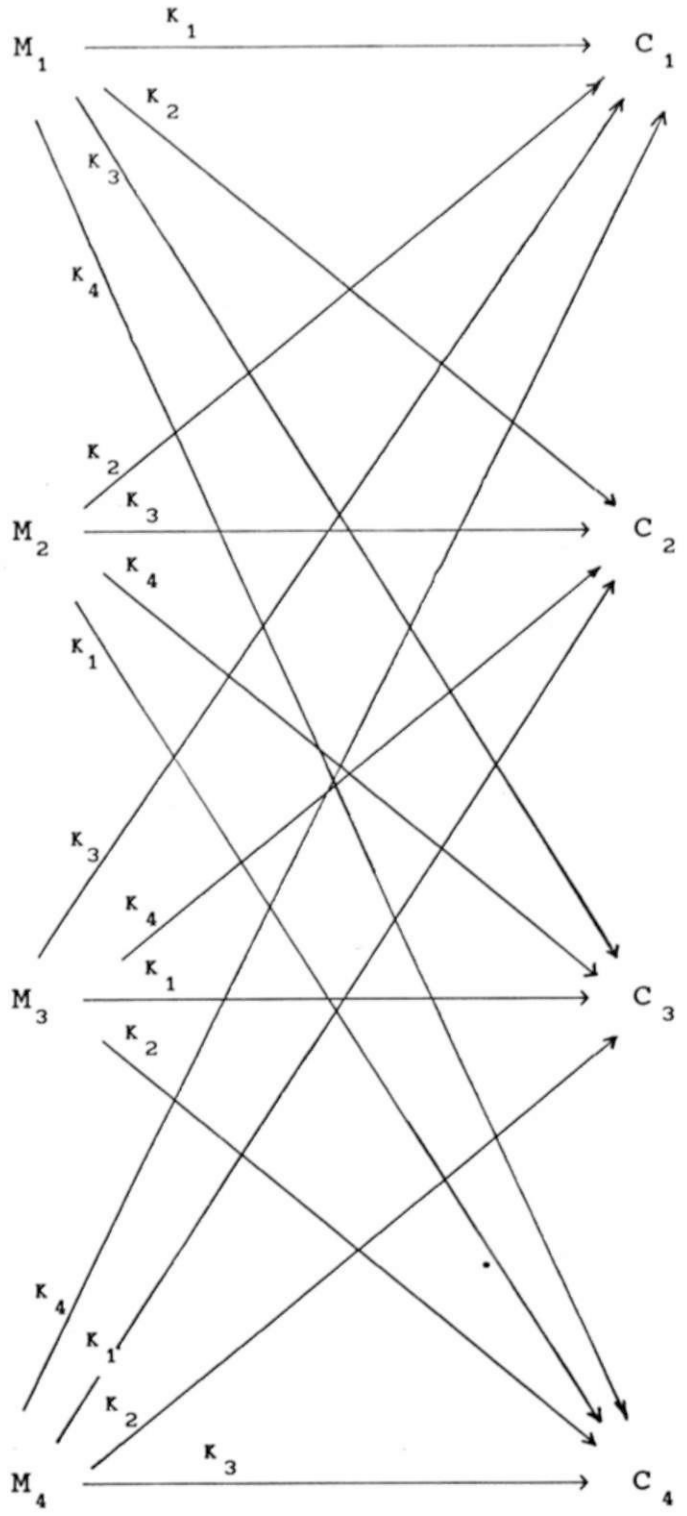



Fig. 2.1 - Sistema de Sigilo Perfeito

Portanto, a condição de sigilo perfeito requer que o número de chaves de cifragem seja pelo menos igual ao número de mensagens, que essas chaves sejam utilizadas de forma aleatória e que o tamanho dessas seja maior ou igual ao tamanho da mensagem que irá ser cifrada. As únicas cifras de sigilo perfeito são as "one-time pad" [8].

## 2.4 - CRIPTOSISTEMAS CLÁSSICOS

Nos algoritmos criptográficos convencionais (clássicos) é empregada apenas uma chave, a qual é utilizada tanto na cifragem dos dados a serem transmitidos como na decifragem dos mesmos. O conhecimento dessa chave é que permitirá que qualquer pessoa cifre ou decifre uma determinada mensagem. O transmissor e o receptor de uma dada mensagem cifrada compartilham a mesma chave criptográfica, através de um canal seguro. Para que a segurança dos dados seja preservada essa chave compartilhada deve ser enviada por meios seguros, tais como, carta registrada, mensageiro confiável, encontros pessoais, etc, e, posteriormente, mantida em sigilo absoluto [12].

De um modo geral, nos sistemas criptográficos, procura-se privacidade e autenticidade. Com a privacidade, requer-se que a obtenção da informação por um indivíduo não autorizado, a partir de uma mensagem cifrada transmitida por um canal inseguro, seja impossí. vel, senão bastante difícil. Assim, uma pessoa que envie uma mensa gem terá certeza que apenas a pessoa desejada (autorizada) será ca paz de ter acesso a essa mensagem.

Na figura 2.2, tem-se um modelo do sistema de comunicação convencional onde se requer a privacidade da informação transmitida.

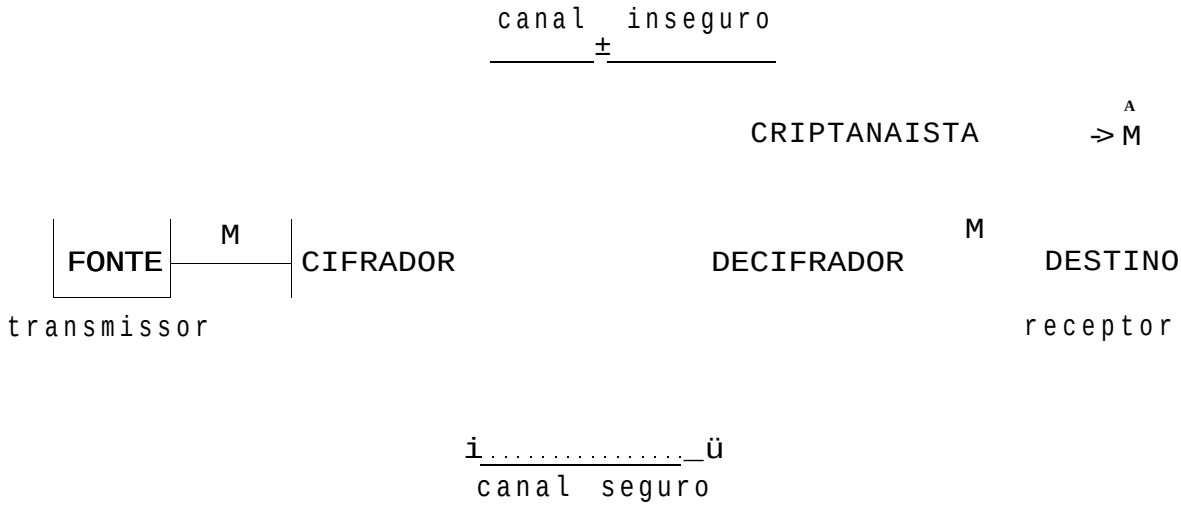



Fig. 2.2 - Sistema Criptográfico Convencional

Observando-se o diagrama da figura 2.2, vêem-se três importantes elementos : o transmissor, o receptor e o criptanalista.

O transmissor gera uma mensagem M a ser enviada, através de um canal bastante inseguro, a um receptor. Para evitar que um indivíduo não autorizado tenha acesso à mensagem M, o transmissor opera em M uma função matemática E, inversível, capaz de codificá-la, obtendo uma mensagem cifrada ou criptograma,

$$C = E_K(M)$$

Essa função E corresponde à transformação de cifragem de uma mensagem clara em um texto cifrado.

Observa-se que a chave K, compartilhada por meio de um canal seguro, é única, e uma vez que é conhecida pelo receptor, este pode decifrar o criptogram C pela obtenção do operador inverso, $E'$, obtendo assim, a informação original a ele enviada, isto é,

$$E'^{-1}(C) = E_r^{-1}(E_r(M)) = M$$

Como a mensagem cifrada é enviada através de um canal inseguro, qualquer indivíduo não autorizado pode ter acesso ao mesmo e obter o texto cifrado C. Poder-se-ia pensar em um canal seguro

para se enviar M, mas assim sendo não teria sentido a cifragem dessa mensagem.

O nível de segurança, que as partes envolvidas na comunicação precisam, pode conduzir à necessidade de autenticidade, a qual requer que alguém não autorizado não seja capaz de introduzir uma nova mensagem ou alterar aquela que está sendo enviada. Na figura 2.3, tem-se um modelo onde se observa a autenticidade.


Fig. 2.3 - Sistema Criptográfico com Autenticidade

O receptor verdadeiro, nesse caso, protege-se de estar sendo enganado por uma mensagem alterada ou introduzida, decifrando to

das as mensagens que recebe, mas aceitando apenas aquelas cifradas com a chave correta [2].

Um sistema com autenticidade é realmente seguro quando não é possível obter-se M a partir de C sem a chave correta K, sendo tam bém impossível criar um criptograma C que, uma vez decifrado com K, produza uma mensagem M' aceita como verdadeira.

De forma geral, com a autenticação, o receptor ou uma ter ceira parte idônea (um árbitro) determina se uma mensagem foi real mente enviada por um transmissor autorizado ou não, em lugar de ter sido um oponente. Dispondo de um protocolo de autenticação, o recep tor aceitará como autêntica apenas uma fração das mensagens recebi das [3].

Qualquer canal pode ser ameaçado por espionagem e/ou intro dução de informações, dependendo apenas da utilização desse canal. Numa comunicação telefônica, por exemplo, a introdução de informa ções é bem mais fácil que a simples espionagem, uma vez que não se pode determinar o fone que está chamando, sendo a espionagem uma téc nica mais difícil e ilegal. Entretanto, numa comunicação via rádio, por exemplo, a situação é a reversa.

Nos sistemas criptográficos convencionais duas técnicas de cifragem são de extrema importância : Substituição e Transposição. Essas técnicas são encontradas como parte integrantes de cifras mais sofisticadas, como as cifras produto. Com estas técnicas criptográfi

cas visa-se ocultar, ou destruir, a frequência relativa dos caracteres de linguagem.

Definição 2.4 - FREQUÊNCIA RELATIVA

A frequência relativa de caracteres em um determinado Idioma corresponde à incidência natural desses caracteres nesse Idioma. Por exemplo, no idioma Português o caracter de maior frequência relativa é o "a", enquanto que no Inglês o caracter é o "e".

Definição 2.5 - CIFRA DE TRANSPOSIÇÃO

Uma cifra de transposição é aquela que rearranja os caracteres do texto claro em uma outra ordem.

Definição 2.6 - CIFRA DE SUBSTITUIÇÃO

Uma cifra de substituição é aquela que muda os caracteres linguísticos de um texto claro por outros caracteres do mesmo ou de outro alfabeto.

Definição 2.7 - CIFRA PRODUTO

É aquela que resulta da composição de t cifras $F_1, \ldots, F_t$, onde cada cifra F pode ser de substituição ou de transposição.

Para efeito de classificação geral, a figura 2.4, reúne as técnicas de cifragem existentes.

- TÉCNICAS CLÁSSICAS DE CIFRAGEM
  - SUBSTITUIÇÃO
    - MONOALFABÉTICA (Cifra de Cesar)
    - HOMOFÔNICA (Cifra de Beale)
    - POLIALFABÉTICA (Vigenère, Beaufort, Vernan)
    - POLIGRÂMICAS (Playfair, Hill)
  - TRANSPOSIÇÃO
    - COLUNAR
      - PERIODICA
- PRODUTO (Máquinas a Rotor, LUCIFER, DES)

Fig. 2.4 - Técnicas de Cifragem

## 4.1 - Cifras de Substituição

1. As cifras de Substituição Monoalfabeticas são aquelas que substituem cada caracter de um alfabeto ordenado *4*, por um outro caracter de um outro alfabeto £ que se apresenta em uma dada ordem.

Alfabeto : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
*4*
Alfabeto : D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Na cifragem da mensagem M = mm.... , teríamos,

$$C = EJM) = f(m_1)f(m_2) \ ...$$

A cifra de Cesar constitui-se num exemplo desse tipo de substituição.

2. A cifra de Substituição Homofônica é aquela que mapeia cada caracter a do alfabeto claro em um conjunto de elementos cifrados f ( a ), chamados homófonos. Uma mensagem M = $^{m}{}_{t}{}^{m}{}_{2}$ ••• é cifrada como C = $c_1 c_2 \ ' \ c_1$ . . . , onde cada c é tomado aleatoriamente

de um conjunto de homófonos f(m). A cifra de Beale, cuja chave foi a Declaração de Independência, é um exemplo desse tipo de técnica de cifragem. Uma vantagem desse tipo sobre a primeira técnica é que os criptogramas produzidos não preservam a estatística das letras do alfabeto original.

3. A cifra de Substituição Polialfabética utiliza ciclicamente, para cada caracter da mensagem, uma substituição distinta que conduza a uma sequência de alfabetos. Nesse caso também, os criptogramas produzidos não preservam a estatística das letras do alfabeto original. Várias são as cifras desse tipo como mostrado na figura 2.3.

4. A cifra de Substituição Poligrâmica é a aquela que cifra blocos de símbolos da mensagem em blocos de texto cifrado, destruindo a frequência relativa dos símbolos do alfabeto original utilizado. Como exemplo, tem-se as cifras de Playfair e de Hill.

## 2.4.2 - Cifras de Transposição

Esse tipo de cifragem normalmente é realizada com o auxílio de alguma figura geométrica, onde através do modo como se põe e se retira o texto pleno dessa figura, consegue-se obter o texto cifrado. Em muitos casos a figura é um arranjo bidimensional, podendo ser contudo de qualquer dimensão.

1. Na transposição de colunas, o texto claro é escrito na matriz por linhas, sendo o criptograma obtido tomando-se as colunas dessa matriz em alguma ordem. Como exemplo, considere uma matriz 3 x 4 e a mensagem M = CRIPTOGRAFIA, logo,

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| C | R | I | P |
| T | 0 | G | R |
| A | F | I | A |

Tomando-se as colunas segundo a ordem 2-4-1-3, tem-se o criptograma

C = ROFPRACTAIGI

Como se vê, para se processar tanto a cifragem como a decifragem, tem-se que gerar toda a matriz.

2. Na permutação com período fixo d, onde sucessivos blocos de caracteres são cifrados, o texto cifrado é obtido permutando se os caracteres de acordo com uma função $f: Z_d \rightarrow Z_d$, que define uma permutação.

   Por exemplo, seja a chave de cifragem K = (d,f) = (4,f(i)) onde f(i): 2 4 1 3 para i = 1 2 3 4. Assim, para M = CRIPTOGRAFIA, tem-se

   E (M) = RPCIORTGFAAI

   Cada bloco pode ser cifrado e decifrado independentemente.

### 2.4.3 - Cifras Produto

Esse tipo de cifra emprega a combinação das duas técnicas de cifragem anteriormente mencionadas, transposição e substituição, e é encontrado, por exemplo, nas conhecidas máquinas a Rotor e no

DES. Podemos citar dois exemplos de cifras dessa natureza.

1. A cifra de LÚCIFER, projetada por Feistel da IBM [16], que utiliza uma transformação que aplica alternadamente substituições $S^{\wedge}$ e transposições $P_{j}$, isto é,

$$C = E_{K}(M) = S_{t} \circ P_{t-1} \circ \ldots \circ S_{2} \circ P_{1} \circ S_{1}(M)$$

onde cada $S^{\wedge}$ é uma função da chave K.

2. O algoritmo DES, também desenvolvido pela IBM, onde um bloco de entrada T é transposto sob uma permutação inicial IP, gerando $T_{o} = IP(T)$. Após passar por 16 iterações de uma função f que combina substituição e transposição, faz-se a permutação inversa $IP^{-1}$ originando o resultado final [17].

## 2.5 - CRIPTOSISTEMAS DE CHAVE-PÚBLICA

A noção de chave pública surgiu em uma publicação de Diffie e Hellman [4], em 1976. Nesse trabalho, foi proposto um sistema no

qual o transmissor e o receptor usariam chaves diferentes, uma para cifragem e outra para decifragem das mensagens. Uma das chaves precisava ser mantida em segredo enquanto que a outra, que apesar de distinta se encontra relacionada com a primeira chave, seria feita de conhecimento público, sem que isto implicasse em comprometimento da segurança do sistema. Esse tipo de sistema pode ser classificado como assimétrico, por usar duas chaves, fornecendo comunicação segura em apenas um sentido [18].

Com o criptosistema de chave pública, tornou-se desnecessário o extremo cuidado no repasse de uma chave secreta única entre os indivíduos A e B, como acontece nos sistemas convencionais de criptografia. Ficou estabelecido, assim, naturalmente, um canal de comunicação mais seguro entre esses dois indivíduos.

### 2.5.1 - Cifragem e Decifragem

Na cifragem das informações, utiliza-se um algoritmo E e uma chave de cifragem ke, enquanto na decifragem, um algoritmo D e uma chave de decifragem kd, são usados. Ambos os algoritmos são de conhecimento público e possuem quatro propriedades básicas:

1. A decifragem da forma cifrada da mensagem M conduz à própria mensagem, isto é,

$$D(E(M)) = M$$

2. Ambos os algoritmos E e D são de fácil computação.

3. Pela revelação do algoritmo E não se revela um meio fácil de se computar D.

4. Se uma mensagem M é primeiro decifrada e depois cifrada, obtem-se de qualquer forma, como resultado, M

$$E(D(M)) = M$$

Essa quarta propriedade está relacionada com a inversibilidade.

Uma função que satisfaça à terceira propriedade, fará com que o número de mensagens a serem testadas pelo criptanalista fique imenso, e, portanto, impraticável. Além disso, uma função que satisfizer às três primeiras propriedades, é dita ser uma função unidirecional com alçapão e se, finalmente, satisfizer à quarta proprieda

de, é dita ser uma função de permutação unidirecional com alçapão.

Definição 2.8 - FUNÇÁO UNIDIRECIONAL

Uma função f é dita unidirecional se é fácil de ser computada em uma direção mas, aparentemente, é muito difícil de ser computada na outra direção, ou seja sua inversa $f^{-1}$ não é trivial [1], [19].

Definição 2.9 - FUNÇÁO COM ALÇAPÁO

Uma função f é dita ser uma função com alçapão se:

1) f é fácil de ser computada em uma direção; e
2) Existe alguma informação adicional (uma chave) sem a qual f é uma função unidirecional, e com a qual é fácil se computar $f^{-1}$ [1],[19].

Quando uma função alçapão satisfaz à quarta propriedade significa que toda mensagem é um criptograma de alguma outra mensagem, além disso, que todo texto cifrado é em si uma mensagem clara. Essa propriedade será apenas necessária quando se precisar de autenticidade.

Na figura 2.5, tem-se o diagrama de blocos de um sistema de chave pública.

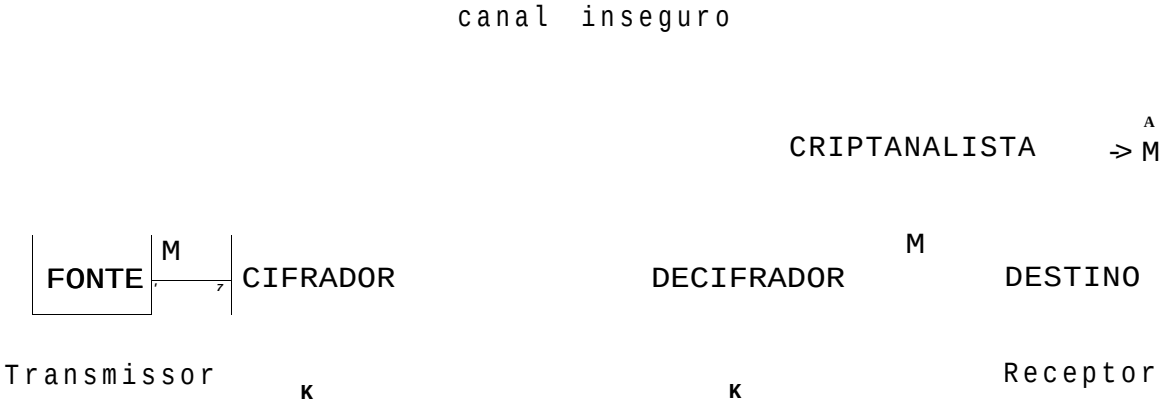



Fig. 2.5 - Sistema Criptográfico de Chave Pública

Na figura 2.6 vê-se um diagrama mais detalhado de um sistema de chave pública.

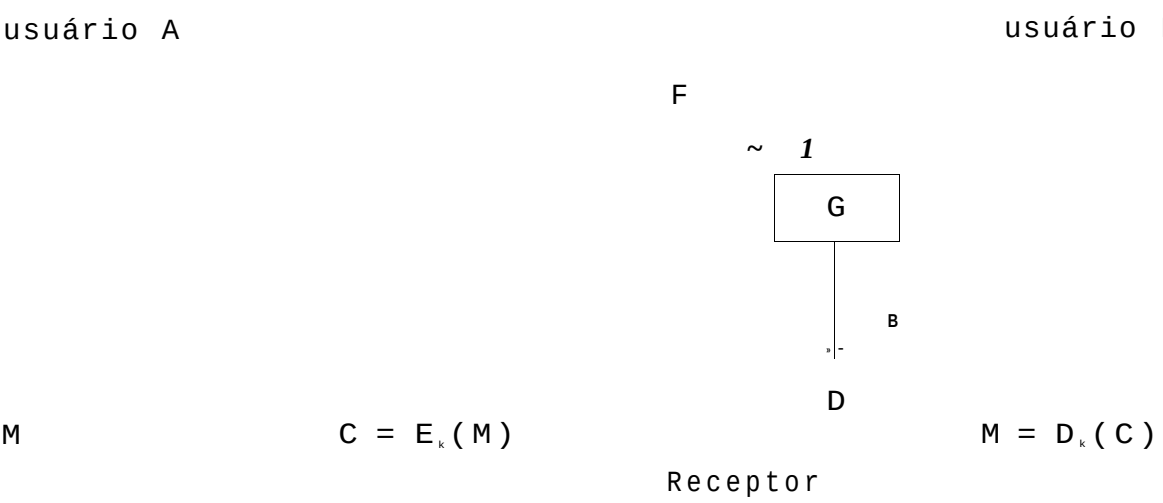



Fig. 2.6 - Diagrama de um Detalhado Sistema de Chave Pública

Como existe um universo grande de chaves, observa-se na figura 2.6 a existência de dois outros algoritmos públicos F e G que são utilizados para gerar, a partir de uma chave k , aleatoriamente escolhida, as chaves de cifragem pública e decifragem secreta, respectivamente, $k_{©B}$ e $k_{uB}$ Mostra-se neste diagrama apenas a comunicação em um sentido, ou seja, o usuário B cria as suas duas chaves, e o usuário A, a partir da chave pública de B, pode apenas enviar-lhe mensagens. A mesma estrutura do gerador de chaves, encontra-se também relacionada com o usuário A.

Por efeito de segurança, as operações de F, G e D, do recep

tor, devem ser mantidas em um micro-chip e o valor $k_B$ não deve estar armazenado neste.

Segundo o diagrama da figura 2.6 , tem-se garantido a privacidade no envio de mensagens por um canal de comunicação inseguro. Contudo, por exemplo, qualquer pessoa, a partir do $k_B$, pode enviar mensagens a B, mesmo sendo um inimigo. Assim, B não tem certeza de quem enviou a mensagem recebida. Surge então a necessidade de se garantir a autenticidade das mensagens. Uma das formas de se obter isto, em um sistema de chave pública, é a assinatura digital.

Uma assinatura digital constitui-se em uma propriedade secreta de um usuário ou processo, que é usada para assinar mensagens. Considere B como o receptor de uma mensagem M que seja assinada por um indivíduo A. Assim sendo, a assinatura de A deve satisfazer:

1. O usuário B deve ser capaz de validar a assinatura de A na mensagem M.

2. Deve ser impossível a qualquer um, inclusive o próprio B, forjar a assinatura de A.

3. No caso em que A negue sua assinatura em M, deve ser possível a um juiz resolver a possível disputa entre A e B.

## 2.5.2 - Principais Criptosistemas de Chave Pública

Os principais criptosistemas de chave pública são os seguintes:

1 - Criptosistema de Diffie-Hellman (Exponenciação Discreta)
2 - Criptosistema de McEliece (Códigos Goppa)
3 - Criptosistema de Merkle-Hellman (Mochila com Alçapão)
4 - Criptosistema de Rivest-Shamir-Adleman (RSA)

Dentre esses sistemas de chave pública estão aqueles baseados no problema do logaritmo discreto e os que se baseiam no problema da mochila.

Definição 2.10 - O PROBLEMA DO LOGARÍTMO

Dados *a*, /3 e um primo p, o problema consiste em se determinar um inteiro x tal que satisfaça à relação

$$a^{x} = \& \pmod{p}$$

Definição 2.11 - O PROBLEMA DA MOCHILA

Dado um inteiro N e um vetor $a = (a_0, a_1, \ldots, a_{n-1})$ o problema consiste em se achar uma solução $x = (x_0, x_1, \ldots, x_{n-1})$, tal que $x_i = 0$ ou 1, $0 \leq i < n$, para a equação

$$N = \sum_{i} a_i x_i$$

O criptosistema de chave pública da mochila com alçapão baseia-se na segunda definição e será tratado no capítulo 3, enquanto o criptosistema RSA que se baseia numa variação da definição 2.10, e que pode garantir privacidade e autenticidade, será tratado no capítulo 4.

## 2.5.3 - Criptosistema de Diffie-Hellman

Quando Diffie e Hellman introduziram as bases para os criptosistemas de chave pública, sugeriram um algoritmo onde se utiliza a exponenciação módulo de um primo p, que seria computada no campo de Galois GF(p).

Considere um primo p e $\alpha$ um elemento primitivo de GF(p). Su

ponha que um indivíduo A deseje se comunicar com um indivíduo B; então A deve escolher um número $X_A$ aleatoriamente distribuído entre os inteiros {1, 2, ... , p - 1}, que deve ser mantido em segredo, devendo ser mantido em arquivo público o número Y^ , constando o nome e endereço de A, dado por

$$Y^{} = a \pmod p$$

Da mesma forma, o indivíduo B escolhe um número $X_B$ que será mantido secreto, e computa $Y_B$, dado por

$$Y_B = a^{X_B} \pmod p$$

o qual é deixado em arquivo público. Quando A e B desejam se comunicar utilizam

$$K_{AB} = a^{X_A X_B} \pmod p$$

que será utilizado como chave. O indivíduo A determina $K_{AB}$ elevando $Y_B$, recebido do arquivo público, à potência $X_A$, ou seja,

$$K_{AB} = (\alpha^{X_B})^{X_A} \pmod p$$

$$= \alpha^{X_A X_B} = \alpha^{X_B X_A} \pmod p$$

o mesmo devendo acontecer com o indivíduo B.

Se p for um primo com aproximadamente 1000 bits, serão necessarias 2000 multiplicações com números dessa ordem de bits, ou seja, $2*\log_2 p$ multiplicações para se determinar $Y_A$ a partir de $X_A$ ou $K_{AB}$ a partir de $Y_A$ e $X_B$. Se um outro indivíduo desejar obter $K_{AB}$ a partir de $Y_A$ e $Y_B$, terá que determinar o logaritmo discreto de $Y_A$ ou $Y_B$, ou seja,

$$K_{AB} = Y_A^{X_B} \pmod p$$

Contudo, tomando-se os logaritmos sob GF(p), são necessárias mais de $2^{-b/2}$ ou $p^{1/2}$ operações, o que nos leva a afirmar que a segurança desse criptosistema baseia-se na dificuldade do problema do logaritmo discreto.

## 2.5.4 - Criptosistema de McEliece

Trata-se de um criptosistema que se baseia em códigos corre

tores de erro, introduzido em 1978 por Robert McEliece [9]. McEliece fez uso da existência de uma classe de códigos corretores de erro, a classe dos códigos Goppa [20], para a qual é conhecido um algoritmo de decoficação rápido.

Existe um forte paralelo entre esse sistema e a mochila com alçapão, pois recai num problema NP-completo [A.I]. No criptosistema de McEliece a chave secreta consiste na matriz geradora G do código Goppa, de ordem k x n, que corrige t erros; em uma matriz não singular S de ordem k x k; e em uma matriz de permutação P de ordem n x n. As matrizes S e P são usadas para alterar a matriz geradora G, gerando a matriz G' dada por

$$G' = S \times G \times P$$

que corresponde à uma matriz geradora k x n de um código linear. Em síntese, tem-se:

Chave Pública : G' = SGP
Mensagem : um vetor k-dimensional m sobre GF(2)
Cifragem : C = mG' + z onde z é um vetor aleatoriamente escolhido sob GF(2) com peso de Hamming no máximo t.

Decifragem : Seja $C = CP^{-1}$. Utilizando-se o algoritmo de decodificação do código Goppa, acha-se m' tal que $d_H(m'G', C) * t$, onde $d_H(u,v)$ representa a distância de Hamming entre u e v. Então, $m = m'S^{-1}$.

McEliece sugeriu que para n = 1024, t seria 50. Segundo Diffie [21], o criptosistema de McEliece nunca alcançou ampla aceitação e tão pouco foi considerado para implementação em qualquer aplicação real. Apesar disso, as cifras baseadas em códigos corretores de erro continuam a despertar o interesse dos pesquisadores na área e, recentemente, novas cifras de chave secreta baseadas em códigos algébricos foram propostas [22].

## 2.6 - CRIPTANÁLISE

Até o surgimento dos computadores digitais a tarefa de decifragem dependia apenas da habilidade humana, sendo mais uma arte. Em todos os métodos clássicos, a análise do texto cifrado pode ser executada rapidamente. Uma vez que o mecanismo de cifragem é conhecido,

a velocidade de processamento dos computadores permite métodos intei. ramente grosseiros na quebra de cifras clássicas.

Em muitos casos, quando a cifra é conhecida, a chave é encontrada com a interpretação da mensagem, através da busca exaustiva. Entretanto, isso não é conveniente, principalmente se o número de chaves é muito grande.

Definição 2.12 - CIFRA QUEBRÁVEL

Uma cifra é dita ser quebrável se for possível se determinar o texto claro ou a chave, a partir do texto cifrado, ou se determinar a chave a partir do par texto claro/texto cifrado.

Existem três métodos básicos ou classes de ataques aos criptogramas em sistemas convencionais e mais um quarto método adicional em se tratando de sistemas criptográficos modernos.

## 2.6.1 - Métodos de Ataque aos Criptogramas

1. Apenas Texto Cifrado
2. Texto Pleno Conhecido

3. Texto Pleno Escolhido

4. Texto Cifrado Escolhido

A criptografia moderna utiliza todos os quatro métodos acima mencionados, enquanto a clássica apenas os três primeiros. Faremos uma rápida abordagem sobre esses métodos de ataque criptanalítico.

No ataque com apenas texto cifrado conhecido, tenta-se determinar a chave interceptando-se o criptograma, embora se possa ter o conhecimento do método de cifragem, do idioma em que se encontra o texto original, de que versa o criptograma e até das palavras mais prováveis de estarem presentes. Se não houver redundância no texto original, fica praticamente impossível se determinar a chave.

No ataque por texto pleno conhecido a tarefa de se determinar a chave é, em geral, menor. Sabem-se alguns pares texto pleno/texto cifrado e, em muitos casos, o conhecimento de palavras provaveis facilita o trabalho de criptanálise. Programas cifrados, por exemplo, são bastante vulneráveis.

No ataque por texto pleno escolhido, um criptanalista é capaz de obter um criptograma correspondente ao texto selecionado. Um exemplo seria um sistema de base de dados.

Finalmente, no ataque por texto cifrado escolhido, embora o

texto pleno não seja provável de ser compreensível, pode-se utiliza lo para se deduzir a chave.

Atualmente,em qualquer caso, com a utilização de recursos computacionais mais sofisticados a tarefa do criptanalista tem sido facilitada.

Neste capítulo, teve-se a oportunidade de se ver que os princípios criptográficos eram de conhecimento milenar e que, atual mente, a criptografia se encontra presente em todas as comunicações onde se vise privacidade e autenticidade. Exemplo disso vemos no trá fego de comunicações de dados entre computadores, nos sistemas de di gitalização de voz, nas aeronaves, na cifragem dos sinais de televi. são, nos facsímile, nas comunicações de satélites, nas transações fi nanceiras e comerciais, nas áreas de crédito bancário, dentre outras áreas que estão despertando para o uso da criptografia e outras que ainda não o fizeram [1], [12], [23].

De modo genérico, as pesquisas em criptologia sempre foram e ainda são conduzidas a portas fechadas. Só a aproximadamente uns 12 anos ficou difundida a pesquisa aberta, mas sempre essa área se constituirá em um assunto conflitante. A pesquisa aberta é uma ques tão onde a mantenabilidade do conhecimento depende, justamente, das trocas de idéias entre os estudiosos da área, principalmente, em en contros científicos ou através de publicações.

# REFERÊNCIAS BIBLIOGRÁFICAS

[1] J. L. Massey, "An Introduction to Contemporary Cryptology", Proceeding of the IEEE, vol. 76, n. 5, pp. 533-549, Maio 1988.

[2] W. Diffie e M. E. Hellman, "Privacy and Authentication : An Introduction to Cryptography", Proceedings of IEEE, vol. 67, n. 3, pp. 397-427, Março 1979.

[3] Gustavus J. Simmons, "A Survey of Information Authentication", Proceedings of the IEEE, vol. 76, n. 5, pp. 603-620, Maio 1988.

[4] W. Diffie e M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, vol. IT-22, n. 6, pp. 644-654, Nov. 1976.

[5] D. E. Robling Denning, "Cryptography and Data Security", Addison Wesley, 1982.

[6] D. B. Newman, Jr e R. L. Pickholtz, "Cryptography in the Private Setor", IEEE Communications Magazine, vol. 24, n. 8, pp. 7-10, Agosto 1986.

[7] S. Pohlig e M. Hellman, "An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance", IEEE Transactions on Information Theory, vol. IT-24, n. 1, pp. 106-110, Jan. 1978.

[8] R. L. Rivest, A. Shamir e L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Criptosystems", Communications of the ACM, vol. 21, n. 2, pp. 120-126, Fev. 1978.

[9] R. J. McEliece, "A Public Key Cryptosystem based on Algebraic Coding Theory", JPLDSN Progress Rep. 42-44, pp. 114-116, Jan-Fev. 1978.

[10] A. Shamir, "A Polynomial-Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem", IEEE Transactions on Information Theory, vol. IT-30, n. 5, pp. 699-704, Srt. 1984.

[11] E.F. Brickell, "Breaking Iterated Knapsacks", Proceedings of Crypto '84, pp. 342-358, Berlim, 1985.

[12] J. K. Omura, "Novel Applications of Cryptography in Digital Communications", IEEE Communications Magazine, pp. 21-29, Maio 1990.

[13] D. Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete", Communications of the ACM, vol. 28, n. 10, pp. 1030-1044, Out. 1985.

[14] Hans-Peter Königs, "Cryptographic Identification Methods for Smart Cards in the Process of Standardization", IEEE Communi. cations Magazine, pp. 42-48, Junho 1991.

[15] James L. Massey, "The Relevance of Information Theory to Modern Cryptography", Proceedings of the 1990 Bilkent International Conference on New Trends in Communication, Control and Signal Processing (BILCON'90), Julho 1990, Ankara, Turquia.

[16] H. Feistel, "Cryptography and Computer Privacy", Sci. Am., vol. 228, n. 5, pp. 15-23, Maio 1973.

[17] M. E. Smid e D. K. Branstad, "The Data Encryption Standard: Past and Future", Proceedings of the IEEE, vol. 76, n.5, pp. 550-558, Maio 1988.

[18] D. W. Davies e W. L. Price, "Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Eletronic Funds Transfer", John Wiley & Sons, 2nd. ed., 1989.

[19] Alan G. Konheim, "Cryptography: A Primer", John Wiley & Sons, 1981.

[20] F. J. MacWilliams e N. J. A. Sloane, "The Theory of Error Correcting Codes", North-Holland, 1986.

[21] W. Diffie, "The First Ten Years of Public-Key Cryptography", Proceedings of the IEEE, vol. 76. n. 5, pp. 560-576, Maio 1988.

[22] T. R. N. Rao e K. H. Nam, " Private-Key Algebraic-Code Encryptions ", IEEE Transactions on Information Theory, vol. IT 35, n. 4, pp. 829-833, Julho 1989.

[23] G. J. Simmons, "Cryptology", Enciclopédia Britânica, ed. 16 , pp. 913-924B, 1986.

# CAPITULO III

## O ALGORÍTMO DA MOCHILA

O criptosistema de chave pública proposto por Merkle e Hellman [1]/ consiste na aplicação de uma função de transformação unidirecional com alçapão a uma sequência de inteiros positivos que constitui o problema clássico conhecido por mochila.

O problema da mochila é bastante conhecido em análise combinatória e acredita-se ser, em geral, de grande dificuldade. Este tipo de problema é dito ser um problema NP-completo [A.I],cuja solução não se dá em tempo polinomial, isso avaliado quando se utiliza qualquer computador determinístico [2].

Através do uso de uma função unidirecional com alçapão, o que se pretende é modificar a estrutura original da sequência de números inteiros que constitui a mochila, dificultando sua obtenção por um usuário indesejado. A essa variação da mochila clássica, chamou-se de mochila com alçapão.

Hellman e Merkle, com o objetivo de esconder ainda mais a estrutura da sequência originalmente projetada, dificultando o problema de sua possível determinação, aplicaram várias transformações multiplicativas modulares de forma iterativa. Esta mochila multi-iterativa, bem como a mochila com alçapão mais simples, a de apenas uma

iteração, sofreram, em 1984, seus primeiros ataques criptoanalíticos aceitos pela comunidade científica [3] [4]. O ataque criptoanalítico, entretanto, sempre se constituirá em um problema em aberto, pois dependerá dos recursos de que disponha o criptanalista.

## 3.1 - DESCRIÇÃO DO ALGORÍTMO

Suponhamos a existência de "n" elementos de pesos conhecidos, dos quais um subconjunto com "1" elementos é colocado em uma mochila, constituindo uma sequência de pesos, cujo somatório se conhece. Esses n elementos constituirão a chave de cifragem de uma da da informação que se deseje enviar. Cada elemento $a_i$ da mochila pertence ao conjunto IN. O problema da mochila consiste em, conhecendo se a soma S dos pesos desse subconjunto de elementos, determinar quais daqueles pesos originaram a soma S. Assim, deseja-se encontrar um vetor binário, $x = (x_1, x_2, ..., x_n)$ onde $x_i \in \{0, 1\}$, tal que o valor S seja resultante do produto interno $a.x$, onde $a = (a_1, a_2, ..., a_n)$, ou seja,

$$S = \sum_{i=1}^{n} a_i x_i \qquad (3.1)$$

A solução do problema da mochila requer, em geral, um numero de operações que cresce exponencialmente com o número de elementos do subconjunto de pesos que constitui a chave de cifragem. Entretanto, dependendo da natureza dos pesos $a^{\wedge}$ , a solução x pode ser encontrada de forma extremamente simples. Desta forma, por exemplo, se o vetor a é do tipo a = ( 1 , 2, 4, $2^{n-1}$ ) , obter x é o mesmo que se obter a representação binária de S, um problema trivial. A mesma trivialidade acontece se o vetor a tem suas componentes formando uma sequência super-crescente.

Definição 3.1 - SEQUÊNCIA SUPER-CRESCENTE

Uma sequência super-crescente é aquela em que cada elemento $a_i$ é maior que a soma dos elementos precedentes, ou seja, se para todo i e IN,

$$a_i > \sum_{j=1}^{i-1} a_j \qquad (3.2)$$

No caso de se ter uma sequência super-crescente, x pode ser encontrado facilmente, através do seguinte procedimento:

1) Se o valor de S ^ a , então x = 1, caso contrário x = 0

2) Se para i = n - l , n - 2 , . .., 1

$$S - E\ (Xj\ .\ a_j\ )\ *\ a_i \qquad (3.3)$$
$$j= i+i$$

então, x = 1. Caso contrário, $x$^ = 0.

EXEMPLO 3.1

Seja n = 4, a = (2, 5,11, 35) e S = 42. Então, na determinação de x = (x , x , x , x ), tem-se que:
1 2 3 4

1) S > a , então x = 1
4 4

2) É preciso verificar se

$$(S - \pounds^{4}_{j=i+i}\ x_j\ .\ a_i\ )\ *\ {}_{3\,j}\ ,\ i = 3,\ 2,\ 1.$$

Para i = 3

42 - x . a = 7 < a então x = 0
4 4 3

Para **1** = 2

$$42 - x_4 a_4 - x_3 a_3 = 7 > a_2 \qquad \text{então } x_2 = 1$$

Para i = 1

$$42 - x_4 a_4 - x_3 a_3 - x_2 a_2 = 2 = a_1 \qquad \text{então } x_1 = 1$$

e portanto, x = (1, 1, 0, 1).

///

Com o intuito de dificultar a solução do problema da mochila, Merkle e Hellman desenvolveram um algoritmo de cifragem pública denominada mochila com alçapão [1]. O algoritmo consiste, inicialmente, na escolha aleatória de um vetor a* cujos elementos formem uma sequência super-crescente, sob o qual será aplicada uma transformação de modo a provocar um espalhamento nos valores de suas componentes. O vetor a' gerado é mantido secreto e com o vetor obtido pela aplicação da transformação sob este, é feita a cifragem da mensagem que será enviada por um canal inseguro de comunicação. Para a construção do vetor modificado, Merkle e Hellman propuseram dois metodos, a mochila aditiva e a mochila multiplicativa. Um quadro classificatório é apresentado na figura 3.1. Nosso estudo se encontra concentrado sob a mochila aditiva.

No processo de decifragem, conhecendo-se os valores b e q mantidos em segredo, determina-se o valor R, 1 ^ R < q - i,

$$R = b^{p} \pmod{q} \qquad (3.11)$$

Donde, tendo-se que,

$$b^{p} = (b)^{1}$$

tem-se

$$b^{u} = \prod_{i=1}^{n} (b^{a_i})^{x_i} \qquad (3.12)$$

Assim,

$$R = \prod_{i=1}^{n} p_i^{x_i} \pmod{q} \qquad (3.13)$$

podendo x ser obtido sem dificuldade. Assim uma decifragem eficiente requer apenas o conhecimento da tripla (p, q, b) . Para elucidar o me todo, segue-se um exemplo.

EXEMPLO 3.3

Considere n = 4, o vetor mochila inicial p = (2, 3, 5, 7), a base dos logaritmos b = 131, q = 257 e D = 264.

1) Na geração da chave pública, empregou-se a equação (3.9) resultando no vetor a = (80, 183, 81, 195).

2) A partir da equação (3.11) e do criptograma D, parte-se para decifrar a mensagem, determinando-se o inteiro R equivalente

$$R = 131^{264} \pmod{257}$$

$$R = 15$$

3) A partir da equação (3.13), chega-se a que a informação cifrada corresponde a x = (0, 1, 1, 0), pois R = 3 #5 .

///

A título apenas de exemplificação do método, tomou-se um vetor p pequeno; contudo, na prática um número razoável de componentes é da ordem de n = 100, onde cada componente $p_j$ possui 100-bits. Isso conduz a uma redução na taxa de transmissão de informação, pois o módulo q seria da ordem de 10.000 bits, tendo-se dificuldades na computação do valor R. Desta forma, poder-se-ia pensar em se utilizar p's pequenos que facilitassem a implementação; entretanto, isso levaria o sistema a tornar-se vunerável a ataques [5].

### 3.1.3 - Mochila com Alçapão Aditiva Binária Multi-Iterativa

Com o objetivo de garantir ainda mais a segurança do cripto sistema baseado no problema da mochila com alçapão, pode-se realizar várias transformações iterativamente, ampliando-se cada vez mais o espalhamento da sequência inicial. Para isso, são escolhidos vários pares de transformações (w^m^).

Inicialmente, partindo-se de uma sequência supercrescente $a_{i}$, determina-se os números $w_{i}$ e $m_{1}$ da mesma forma que descrito anteriormente. Através da expressão (3.4), obtem-se numa primeira iteração o vetor $a^{\wedge}$. Na iteração seguinte, serão escolhidos dois outros números $w_{2}$ e $m_{2}$ relativamente primos, de forma que se tenha, novamente pela aplicação da equação (3.4), um novo vetor $a^{\wedge}$. Dessa mesma forma, procede-se iterativamente quantas vezes sejam necessárias de modo a obscurecer a estrutura da chave pública de cifragem. O processo consiste em cifrar a mochila original $a^{\wedge}$ através de repetidas aplicações de uma transformação básica que preserve a estrutura do problema. O vetor resultante final, ou seja, a chave pública se constitui em uma coleção de números aparentemente aleatórios.

A princípio, poder-se-ia pensar que o efeito da repetição da transformação (w,m) fosse semelhante a aplicação de uma transformação composta, por exemplo o mesmo que dois cifradores por substi

tuição. Em se tratando especificamente desses cifradores, a transformação pode ser direta, ou seja, aplicar-se dois cifradores é equivalente a aplicar-se um único cuja função de mapeamento seja semelhante à composição dos mapeamentos individuais dos dois cifradores. Isso porém, não acontece quando utilizamos o par de transformação (w,m), pois a repetição de duas ou mais dessas transformações não é, em hipótese alguma, semelhante à aplicação de uma única transformação [1]. Para melhor elucidar a mochila multi-iterativa apresentamos um exemplo.

EXEMPLO 3.4

Considere n = 4, o vetor mochila inicial $a.^{\wedge}$= (5, 10, 20, 45), e os parâmetros m = 91 e w = 17 ( $w^{-1}$ 75). Considere duas iterações. Desse modo,

1) Primeira iteração. Aplicando-se a relação expressa pela equação (3.4), com o par $(w, m)_{\#}$ tem-se o vetor mochila modificado $a_2$.

$$a_2 = (85, 79, 67, 37)$$

2) Para a segunda iteração, determina-se um novo par de transformação $(w, m)$ de forma que $mdc(w, m) = 1$ e que

m obedeça à equação (3.3). O problema reside em se determinar um par de números relativamente primos que sejam grandes. Seja $w_2 = 3$ ($w_2^{-1} = 181$) e $m_2 = 271$, logo pela aplicação da equação (3.4), tem-se

$a_3 = (257, 237, 201, 111)$.

Está será a chave pública.

3) O indivíduo que deseje enviar, por exemplo, a mensagem $x = (1, 0, 1, 1)$, enviará pelo canal inseguro, segundo a equação (3.6), o criptograma

$$S_3 = a_3 . x = 567$$

4) O valor $S_3$ será decifrado numa primeira vez, pela equação (3.7), como

$$S_2 = w_2^{-1} . S_3 \pmod{m_2}$$
$$S_2 = 189$$

5) Aplicando-se, novamente, a transformação expressa pela equação (3.7), tem-se

$$S_1 = w_1^{-1} . S_2 \pmod{m_1}$$
$$S_1 = 14.175$$

6) Da mesma forma que no exemplo 3.1, determina-se a solução x.

i) $70 \wedge a_4 \quad x_4 = 1$

ii) $70 - 45 = 25$ i $a_3 \quad X_3 = 1$

iii) $70 - 45 - 20 = 5$ 2: $a_2 \quad x_9 = 0$

iv) $70 - 45 - 20 = 5 \wedge a_2 \Rightarrow x_1 = 1$

Assim sendo, tem-se que a informação enviada pelo canal foi $x = (1, 0, 1, 1)$.

///

Com esse exemplo mostramos a criação de uma chave de cifragem com alçapão multi-iterativa e as etapas de cifragem e decifragem de uma informação x.

Neste método iterativo, em cada estágio sucessivo de transformação, necessita-se aumentar, de uma quantidade fixa, o número de bits dos componentes dos vetores mochila intermediários [1]. Assim, se aumentarmos, por exemplo, a cada iteração, 7 bits, ao final de 40 iterações cada $a^{\wedge}$ terá 280 bits a mais que a quantidade de bits que tinha no início.

Seria possível se proceder da mesma forma utilizando-se o

método da mochila com alçapão multiplicativa. Em qualquer caso, uma vez determinada a chave de cifragem, pode-se tornar ainda mais difícil o acesso à sua estrutura original, permutando-se a ordem de seus componentes, publicando, como chave pública de cifragem, essa versão modificada.

## 3.2 - SEGURANÇA DO ALGORÍTMO

A dificuldade associada à criptanálise de uma cifra está na quantidade de recursos financeiros de que se disponha ou no período de tempo necessário a obtenção dessa solução. No caso do criptosistema de Merkle e Hellman, um dos principais problemas diz respeito, no caso da mochila aditiva, à determinação de um par de transformação (w,m), onde mdc(w,m) = 1, formando a tripla (a*, w, m); e, no caso da mochila multiplicativa, à determinação de uma sequência de primos grandes e um par de transformação, de modo a constituir uma tripla (P/fc>,q)•

Na verdade, a segurança de um cifrador depende, em muito, da complexidade computacional do problema em que se baseia. Deve-se ter em mente que nem sempre a dificuldade computacional de um proble

ma garante a segurança do criptosistema. Quanto aos sistemas de chave pública, ainda não se tem em definitivo uma prova completa de sua segurança.

Definição 3.2 - SEGURANÇA IDEAL

A segurança ideal de um criptosistema pode ser definida como aquela em que a complexidade computacional é impraticável quando submetido a qualquer ataque com probabilidade desprezível de quebra.

O trabalho do criptanalista depende do algoritmo e da máquina utilizados. É costume classificar-se a complexidade de um algorítmo em função de tempo e espaço requeridos segundo o tamanho das entradas do sistema, ou seja, em função de um parâmetro n associado ao problema. No caso da mochila, n corresponde ao número de elementos da chave pública de cifragem.

Ainda quanto à avaliação dos algoritmos, muitos critérios são de interesses, mas, normalmente, o que interessa mais é a taxa de crescimento do tempo ou espaço de memória requerido para se obter uma solução do problema. Em geral, à dimensão de um problema costuma se associar um número inteiro.

Definição 3.3 - DIMENSÃO DE UM PROBLEMA

A dimensão de um problema fica definida como a quantidade de dados de entrada de que disponha o problema.

Definição 3.4 - COMPLEXIDADE DE TEMPO

Por complexidade de tempo deve-se entender o tempo requerido por um algoritmo expresso como função do tamanho do problema.

Definição 3.5 - COMPLEXIDADE DE TEMPO ASSINTÓTICA

Por complexidade de tempo assintótica deve-se entender o comportamento no limite, quando a dimensão do problema cresce ao infinito.

De acordo com as definições (3.6) e (3.7), pode-se definir a Complexidade de Espaço e a Complexidade de Espaço Assintótica. Em geral, é a complexidade assintótica dos algoritmos que determina os tamanhos dos problemas a serem solucionados por esses algoritmos. Se um algoritmo processa as entradas de tamanho n em um tempo $cn^2$, onde c é uma constante, diz-se que a complexidade de tempo deste algorítmo é da "ordem de $n^2$ ", ou $0(n^2)$.

Definição 3.6 - ORDEM

Uma função g(n) é dita ser 0(f(n)) se existe uma constante c, tal que g(n) ^ cf(n) para todos os conjuntos finitos de valores positivos de n.

A complexidade de tempo usualmente é interpretada como o número de unidades de tempo necessárias para processar uma entrada de tamanho n. Usualmente, um algoritmo pode ser classificado como possuidor de complexidade polinomial ou exponencial conforme seja a relação do seu tempo de execução em função das entradas do sistema.

Definição 3.7 - COMPLEXIDADE POLINOMIAL E EXPONENCIAL

A complexidade é dita ser polinomial se o tempo de execução do algoritmo for expresso por T = Ofn¹). Enquanto a complexidade é dita ser exponencial se o tempo de execução do algoritmo for expresso por T = 0(t$^{h(n)}$), para um t constante e um polinómio h(n).

Diffie e Hellman, por volta de 1976, observaram que os problemas NP-completo [A.I],eram de grande utilidade para os algoritmos

de cifragem, uma vez que estes algoritmos não podiam ser solucionados em tempo polinomial, com as técnicas conhecidas até aquela época [5]. Contudo, essa classificação não necessariamente se estende ao problema da mochila com alçapão de Merkle-Hellman, cuja existência baseia-se em uma função unidirecional com alçapão.

Merkle e Hellman, inicialmente, como forma de aumentar a complexidade computacional do algoritmo e tornar impraticável computacionalmente a sua quebra, sugeriram uma mochila de tamanho n superior a 100. Entretanto, Schroeppel e Shamir desenvolveram um algoritmo capaz de solucionar o problema da mochila de tamanho n = 100, em tempo da ordem de $0(2^{n/2})$ e em espaço de $0(2^{n/4})$ [1]. Por esta razão, Merkle e Hellman sugeriram a escolha de vários pares (w,m) e a realização de várias transformações, iterativamente. A escolha dos elementos aj do vetor mochila a* é de grande importância, em função de se aumentar a complexidade computacional do algoritmo à proporção em que se trabalha com números grandes e, portante, módulos m também grandes. Desse modo, os componentes a' podem ser escolhidos na faixa de

$$[\ (2^{i-1}-1).2^{n}+1\ ,\ 2^{i-1}\ .\ 2^{n}\ ]$$

fazendo-se com que se tenha $2^{n}$ possibilidades de escolha para cada a . Da mesma forma, deve-se ter cuidado na escolha dos valores do

par de transformação (w,m). O valor de m deve ser escolhido de forma que se preserve a equação (3.5) e que $m > 2a_n$; portanto, na faixa de

$$[\ 2^{2n+1} + 1\ ,\ 2^{2n+2} - 1\ ]$$

O valor da constante multiplicativa w deve se encontrar na faixa de [2 , m - 2], de forma que se tenha mdc(w,m) = 1.

Apesar de todas as precauções recomendadas por Merkle e Hellman, a quebra do algoritmo da mochila aditiva em tempo polinomiai, aconteceu em 1984 com o trabalho de Shamir, para mochilas de apenas uma iteração. Para tanto, Shamir teve como base novos resultados de programação inteira, o algoritmo de Lenstra. Outros autores seguiram o caminho deixado por Shamir na busca da criptánalise do algorítmo de Merkle e Hellman. A mochila com alçapão multiplicativa também foi quebrada em 1984 por Odlyzko [5]. A mochila com alçapão multi-iterativa resistiu até o final de 1984, quando então, Ernie Brickell anunciou a criptanálise dos sistemas baseados em mochilas com até 40 iterações [4].

Na seção seguinte examinaremos a quebra do algoritmo da mochila aditiva, com apenas uma iteração, proposta por Shamir.

## 3.3 - CRIPTANÁLISE DO ALGORÍTMO DE MERKLE-IIELLMAN

Dentre as variações de criptosistemas que empregam o problema clássico da mochila, o algoritmo proposto por Merkle e Hellman [1] parecia ser significativamente menos provável à quebra quando era utilizado o recurso das múltiplas iterações, fato este que não se verificou. Os métodos aditivo e multiplicativo utilizados na obtenção da chave pública de cifragem e esse último recurso citado, realmente, pareciam ser muito eficientes. Muitos autores propuseram ataques ao criptosistema de Merkle e Hellman, porém nenhum mostrou se convincentemente aplicável [6]. Shamir, completando suas investidas [7] e seguindo os caminhos apontados por outros pesquisadores [6], culminou por conseguir a quebra do algoritmo da mochila com aicapão aditiva de uma iteração [3].

De forma semelhante, Odlyzko [5] apresenta um método de quebra, sob certas condições, do criptosistema da mochila multiplicativa de Merkle-Hellman. O problema da segurança da mochila multi-iterativa ainda permanecia em aberto. As pesquisas quanto aos ataques continuaram após Shamir, até que Merkle chegou a oferecer $ 1.000 àquele que conseguisse quebrar a mochila multi-iterativa, até então, em 1984, tida como segura. Nessa época, Ernie Brickell [4] anunciou a quebra do criptosistema da mochila com 40 iterações, para uma mochila com 100 elementos, em aproximadamente uma hora, utilizando-se

para isso do CRAY-1 [2]. Portanto, constatou-se que as transformações iterativas *w (mod m) não aumentam a segurança do criptosistema como pensava Merkle-Hellman. Desmedt-Vandewalle-Govaerts afirmaram este fato [8], registrando que nesta forma de cifragem podem haver três possibilidades: a segurança ficar completamente perdida, uma vez que uma sequência supercrescente poderia ser facilmente obtida; ter-se nível de segurança igual aos sistemas com múltiplas transformações, mesmo se apenas uma transformação for realizada; ou uma segurança alta pode ser obtida. No criptosistema de Merkle e Hellman, tem-se a primeira das três possibilidades sob o ponto de vista teórico.

### 3.3.1 - Descrição do Algoritmo de Criptanâlise

O algoritmo de criptanâlise da mochila aditiva binária de Merkle-Hellman de apenas uma iteração [3], parece ser de fácil implementação, e até mesmo eficiente em microcomputadores.

Para o ataque, Shamir aplicou os novos resultados do algoritmo de programação inteira de Lenstra, o que permitiu, a partir de uma chave pública a , descobrir um par de inteiros (w',m') capaz de

convertê-la numa sequência supercrescente mantida secreta através da transformação

$$aj = w'.a_{i} \pmod{m'} \quad , \quad i = l, \ldots, n \qquad (3.14)$$

obedecendo de maneira semelhante à expressão (3.5). O criptanalista não necessariamente precisa encontrar, através de algum par (w',m'), uma sequência de números semelhante à que foi originalmente utilizada na construção da chave pública; portanto, este par não precisa ser o original. Através de algum par (W,M) basta que seja suficiente encontrar uma chave de decifragem simples, usando a transformação

$$* \; W \bmod M \quad \text{onde } W = w''^{1} \pmod{M} \qquad (3.15)$$

de forma que mensagens cifradas com o vetor mochila público possam ser decifradas [3], [8]. Isso é possível porque cada $a$^ da chave de cifragem foi obtido a partir de uma sequência simples (supercrescente) por meio de uma multiplicação modular. Procura-se determinar um par (W,M), de forma que a partir da chave pública $(a_1, a_2, \ldots, a_n)$ se possa determinar uma sequência supercrescente aj, a^, a^, obtida através da relação

$$a[ = W.a_{4} \pmod{M} \qquad (3.16)$$

onde as equações (3.2) e (3.5) devem ser respeitadas. A princípio sabe-se que existe pelo menos um par $(W_q, M_o)$, aquele que deu origem à mochila e que portanto, $W_q = w^{-1}$, segundo a expressão (3.15).

É importante observar que todo o ataque será feito diretamente sobre a chave pública e que a complexidade do algoritmo de criptanálise é polinomial em tempo [3]. O criptanalista não precisa encontrar a sequência original.

Na verdade existem alguns pares (W,M) que conduzem a uma sequência supercrescente; o que Shamir fez foi observar como determinar mais facilmente esses pares.

Inicialmente, antes de entrar na questão da obtenção do par (W,M), são necessárias algumas considerações. Dois parâmetros que são de extrema importância são o número de elementos que compõe a chave pública, ou seja, n, e o número de bits de cada elemento dessa chave. Faz-se a suposição, em todo o trabalho, de que o tamanho do módulo Mo utilizado na obtenção da mochila cresce linearmente com o número de elementos da sequência supercrescente, n, isto é,

$$Bits(Mo) = dn \qquad (3.17)$$

onde d representa a constante de proporcionalidade que mede a redundância introduzida pelo criptosistema, ou seja,

$$d = \frac{\text{Bits (Texto Cifrado)}}{\text{Bits (Texto Claro)}} \quad (3.18)$$

Além disso, considerar-se-á que cada elemento da sequência supercrescente aj foi escolhido tal que seu tamanho também dependa do tamanho da chave e da redundância, proporcionando que cada elemento da sequência tenha tamanho distinto, dado por

$$\text{Bits}(aJ) = d\,n - n + i - l \quad (3.19)$$

Com essas observações iniciais, passa-se a análise do algoritmo criptanalítico.

A avaliação do algoritmo proposto por Shamir compreende duas partes, as quais corresponderão a condições para obtenção do par (W,M). Na primeira parte, ter-se-á uma condição de necessidade, onde o algoritmo de programação inteira de Lenstra será utilizado, a fim de se possa encontrar pequenos intervalos pertencentes ao intervalo [0, 1], onde a razão (W/M) e [0, 1]. Na segunda parte, ter-se-á a condição de suficiência, onde, supondo-se que a razão W/M seja aproximadamente conhecida, procura-se refinar a busca do par, dividindo-se cada intervalo encontrado em subintervalos menores, tal que a razão (W/M) pertença a um desses subintervalos. Determina-se, en

tão, com um algoritmo de Aproximação Diofântica [A.II], o menor par (W,M) que satisfaça às condições e que, portanto, determine uma sequência supercrescente.

Para a primeira parte do algoritmo faz-se necessário um estudo da forma gráfica da expressão (3.17) que relaciona a chave pública com a sequência supercrescente, segundo a figura 3.2.

^ a' = Wo.a (mod Mo)

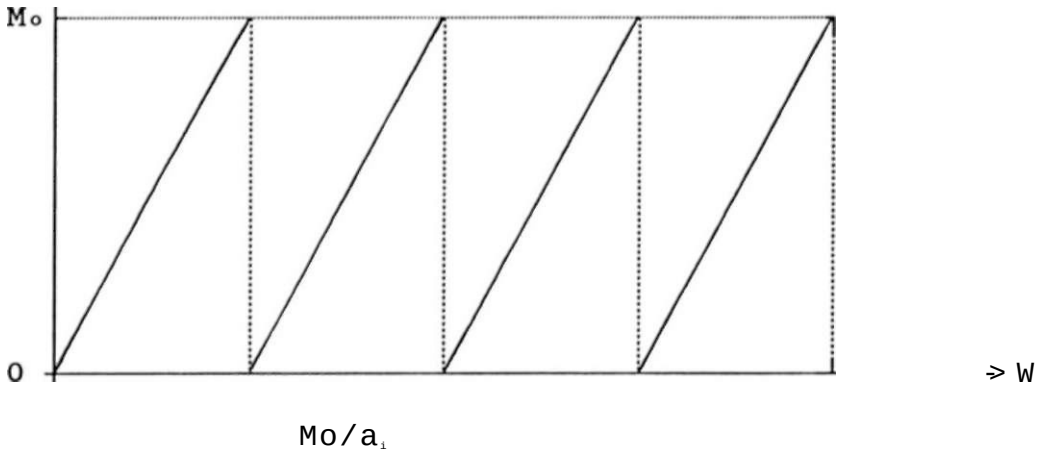



Fig. 3.2 - Curva de Transformação da Sequência Supercrescente

Vê-se facilmente que a inclinação da curva correspondente a

aj , é $a^{\wedge}$ e que existem $a_{(}$ pontos de mínimos que se distanciam um do outro por um valor pouco maior que a unidade, dado pela razão Mo/$a_{j}$.

Segundo a expressão (3.20), o elemento aj da sequência supercrescente será o de menor tamanho e aquele do qual o parâmetro Wo estará mais próximo. Assim, toda a análise é feita com relação à curva associada a este elemento. Através da análise gráfica, determina-se que o parâmetro Wo se encontra a uma distância $2\sim^{n+1-1}$ de um mínimo da curva aj. Como o par (Wo,Mo) que originou o elemento $a^{\wedge}$ originou todos os demais elementos, deve-se tentar fazer uma relação, através de uma superposição, com todas as curvas dos a^s. O parâmetro Wo deve se aproximar simultaneamente de todos os mínimos das curvas superpostas na análise e, portanto, o melhor será trabalhar com os pontos de acumulação das várias curvas. Porém, como normalmente, para efeito de segurança, trabalha-se com chaves com um número grande de elementos, torna-se absurda a idéia de se trabalhar com todas as curvas simultaneamente, a fim de se determinar os pontos de acumulação. O que Shamir propôs foi avaliar quantas curvas seriam suficientes para, quando analisadas simultaneamente, fornecerem resultados apreciáveis.

Analisando-se as curvas relacionadas aos elementos de menor tamanho na sequência supercrescente, portanto, as curvas $a'_1$ e $a'_2$, determinou-se que o mínimo da curva a' se situa a uma distância de

$2^{-}$"$*^{1}$ a esquerda e de $2^{n}$ a direita do mínimo mais próximo da curva aj . Essa disposição faz com que a localização do Wo se restrinja a certas regiões, conforme mostra a figura 3.3.

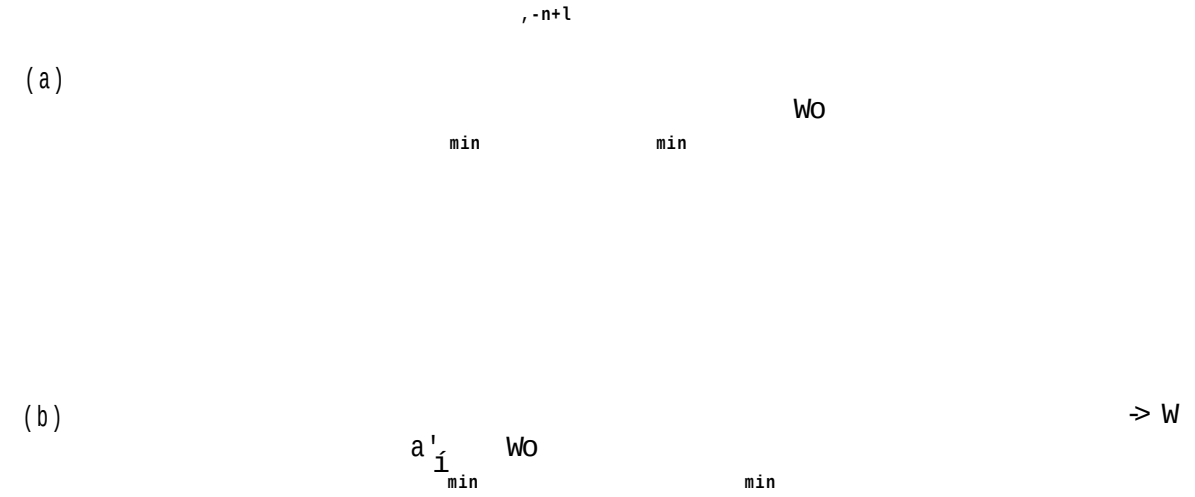



Fig. 3.3 - Localização de Wo

Restou, então, determinar quantas curvas seriam necessárias. Considerando o p-ésimo mínimo da curva aj , determina-se que o mínimo da curva aj mais próximo a este mínimo está no intervalo

I" Mo Mo Mo Mo "1 ...

Supõe-se, então, que as localizações dos mínimos das curvas aj comportam-se como variáveis aleatórias independentes com distribuição de probabilidade uniforme naquele intervalo.

Considerando-se *1* curvas, determina-se que a probabilidade de que os mínimos dessas curvas estejam próximos do p-ésimo mínimo da curva a'í é

$$P(a_2 r a_3 / \bullet\bullet\bullet \# a\ j) = 2 \quad .2 \ . \ . \ . \ . 2 .$$

$$P(a_2, a_3, \ldots, a_j) - 2^{2} \qquad (3.21)$$

Porém, como a curva aj dispõe de $a^{\wedge}$ pontos de mínimos, então o número médio de pontos de acumulação nessas curvas é

$$a^{\wedge}{}_2 - l n_+ n_+ l^2 / 2 \ m_2 d n - l n_+ n_+ l^2 / 2 \qquad (3.22)$$

Para que o número médio de pontos de acumulação seja menor ou igual a 1, deve-se ter,

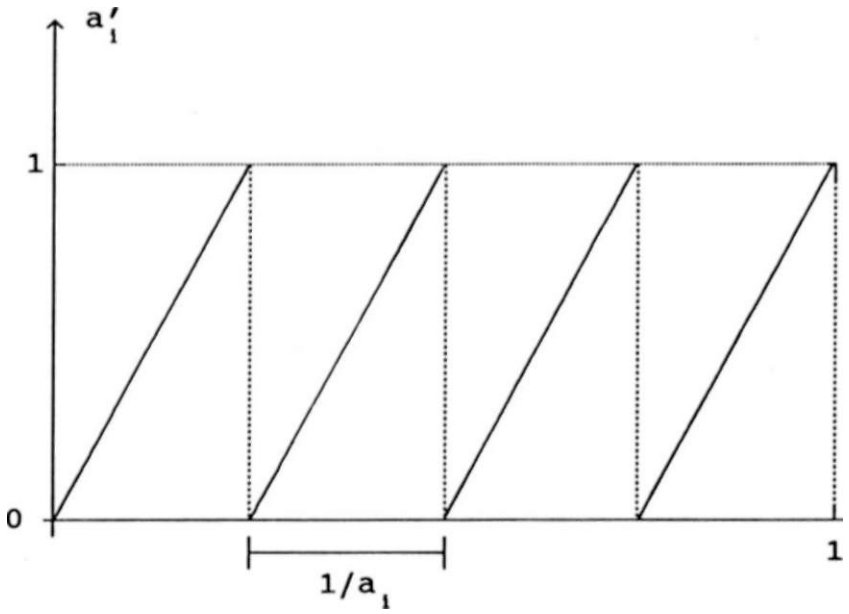
$$(1 - d - l) n > l^2 / 2 \qquad (3.23)$$

donde, supondo-se que n seja muito grande, chega-se a que o número

de curvas a serem analisadas independe do número de elementos da chave pública de cifragem, ou seja,

$$1 > d + 1 \qquad (3.24)$$

Contudo, ao se determinar o número de curvas a serem analisadas não se solucionou o problema do desconhecimento do módulo Mo, nem se determinou os pontos de acumulação dessas *1* curvas. Para se eliminar o problema do módulo, normaliza-se a curva correspondente a cada a', dividindo-se pelo módulo Mo, obtendo-se, assim, uma nova curva, figura 3.4,




» V

Fig. 3.4 - Curva Normalizada

Essa divisão por Mo, não altera a inclinação ou o número de pontos de mínimo da curva a|. O parâmetro Wo será substituído por Vo = Wo/Mo. A distância entre Wo e o mínimo da curva aj mais próximo, será reduzido por $2^{dn}$, ou seja

$$^{-n+i-1} \rightarrow 2^{-dn-n+1-1} \qquad (3.25)$$

Quanto à localização dos pontos de acumulação das *1* curvas no novo sistema de coordenadas (fig. 3.4), passa-se a descrevê-los por um sistema de desigualdades lineares onde se deseja que o p-ésimo mínimo de $a'_1$, o q-ésimo mínimo de $a'_2$, o r-ésimo mínimo de $a'_3$, etc..., estejam o mais próximo possível. O sistema de desigualdades lineares é expresso por

$$\begin{array}{lll} P, q, r & \text{inteiros} & 1 * p * a - 1 \\ -\hat{O}_2 < pa_{*2} - qa_{*1} s \hat{o}'_2 & & 1 * q * a_2 - 1 \\ -\hat{o}_3 < pa_3 - ra_1 \text{ í } <5'_3 & & 1\ 3\ r\ s\ a_3 - 1 \end{array} \qquad (3.26)$$

A partir dessas equações, utiliza-se o algoritmo de programação inteira de Lenstra para se saber se o sistema de desigualdades lineares possue solução inteira. Determinando-se assim, um intervalo pertencente a [0,1], tal que uma condição necessária para que se tenha um par (w',m') é que a razão w'/ m' esteja também neste intervalo. Em seguida, passa-se à segunda parte do algoritmo onde, das regiões encontradas, descartam-se as subregiões nas quais a sequência de valores não proporcionará uma sequência supercrescente, ou então cuja soma de seus valores será menor que a unidade. Esta fase constitue-se no refinamento da análise, onde se procura a condição de suficiência para que haja o par (w',m'), através de um algoritmo de Aproximacão Diofântica.

Supondo-se que p seja um dos valores encontrados através da solução do sistema (3.26), e que pertença a curva a considere o intervalo I entre dois mínimos sucessivos de aj

$$I = |"p/a_{1} , (p + 1)/ al \qquad (3.27)$$

Graficamente, tem-se

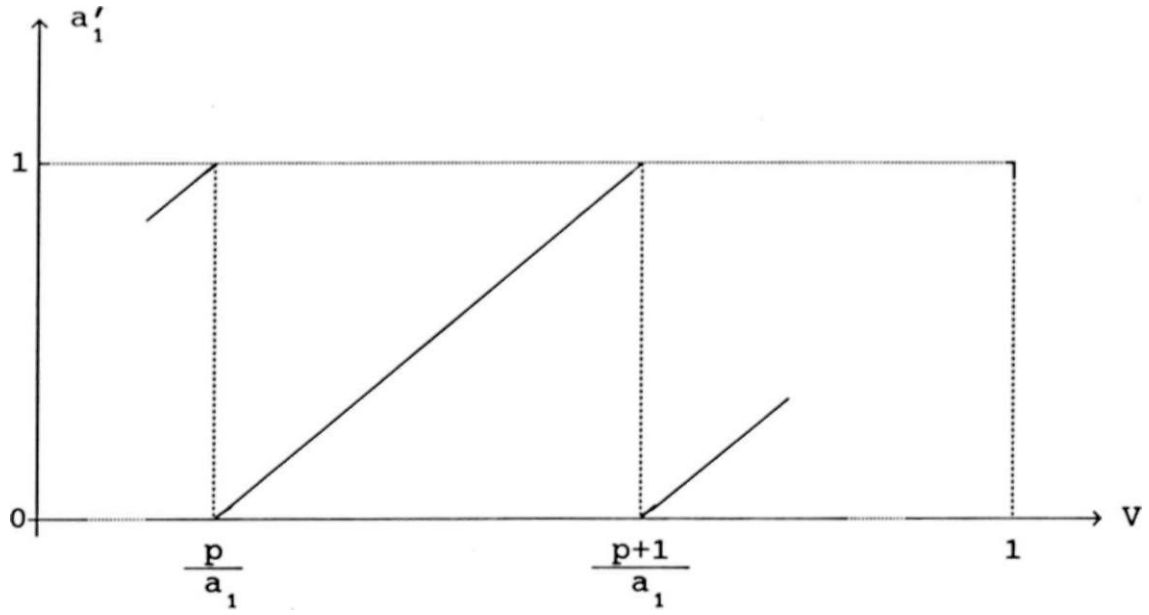



Fig. 3.5 - Intervalo entre Mínimos Sucessivos da Curva a

Nesse intervalo I, tem-se que o número médio esperado de pontos de descontinuidade é 0(n). Esses pontos têm por coordenadas V os valores $V_1, V_2, \ldots, V_t, \ldots, V_s$, arranjados em ordem crescente. Entre quaisquer dois desses pontos de descontinuidade, $V_{rc+}$ e $V_{rc+}$, no intervalo I, todas as curvas a^ se assemelham a segmentos lineares, segundo a figura 3.6.

a í '

-> V

V t +1

Fig. 3.6 - Curva a entre dois Pontos de Descontinuidade

Portanto, tomando-se o i-ésimo segmento linear da curva a , podemos expressá-lo por

Va í - T l í ,, para V t s V < t• V í

onde x' í é o número de mínimos da curva a , í no intervalo (0, V t ], ou seja, T i / a 1 é o ponto da curva que intercepta o eixo V, segundo a fig. 3.6.

Desta forma, para todas as curvas, pode-se escrever a faixa

das coordenadas V, o tamanho correspondente a soma dos segmentos lineares na faixa considerada e as condições para que haja a super Crescência, respectivamente, como

$$v_t * v \leq v_{t+i}$$

(3.28)

$$(va, -r)) > V(v_{aj} -, ;) \quad \text{para } i = 2,3,...,n$$

A solução desse sistema de desigualdades lineares em V, equação (3.28), é um subintervalo de , $v_{t+}$ jj e qualquer valor W/M, neste subintervalo, para algum p e t, é uma condição necessária e suficiente para que W e M sejam uma transformação. Desta forma, tem-se que proceder para todos os pontos solução da equação (3.26), e assim, concluir o algoritmo de busca por um par (W,M) proposto por Shamir.