Criptografia e Álgebra

Rosilaine de Menezes

17 de março de 2003

Agradeço a Deus e aos meus pais por estarem sempre ao meu lado, à professora Cristina Marques pela orientação, paciência e compreensão, e ao Vanderlei pelo amor e incentivo.

Introdução

No decorrer do curso de especialização em matemática, as disciplinas Estruturas algébricas I e II despertaram meu interesse pelas aplicações da álgebra na criptografia.

A criptografia estuda os métodos que podem ser empregados para codificar uma mensagem de modo que apenas seu destinatário legítimo consiga decodificá-la. É uma área que vem se desenvolvendo rapidamente, sendo usada hoje, principalmente na proteção de informações que trafegam através de canais inseguros de comunicação como, por exemplo, a internet.

Assim, ao solicitar à professora Cristina Marques que me orientasse neste trabalho, pretendia investigar como a álgebra é utilizada para assegurar o sigilo das informações. Nesse sentido, no primeiro capítulo retomo alguns conceitos associados às estruturas algébricas: anéis e grupos. No segundo capítulo, faço um levantamento dos principais fatos ligados à evolução da criptografia. Já nos dois últimos capítulos são ilustrados alguns sistemas criptográficos, nos quais conceitos da álgebra são aplicados na codificação, decodificação e análise da segurança de dados.

Sumário

Lista de Tabelas

Lista de Figuras

Capítulo 1

Preliminares

Encontramos na criptografia aplicações interessantes das estruturas algébricas anéis e grupos. Para que possamos compreender melhor o uso de tais estruturas no decorrer deste trabalho, dedicaremos este capítulo à uma breve revisão.

1.1 Anéis

Definição 1.1.1 *Denominamos* ***anel*** A *um conjunto dotado de duas operações, adição e multiplicação, cujos elementos satisfazem as seguintes condições:*

i. (Comutatividade da soma) *Para todo* a *e* $b \in A$*, temos* $a + b = b + a$*.*

ii. (Associatividade da soma) *Para todo* a*,* b *e* $c \in A$*, temos* $(a + b) + c = a + (b + c)$*.*

iii. (Elemento neutro da adição) *Existe um elemento* $0 \in A$ *tal que* $a + 0 = a$ *para todo* $a \in A$*.*

iv. (Elemento simétrico) *Se* $a \in A$*, então existe um elemento* $b \in A$ *tal que* $a + b = 0$*. (Notação: o simétrico de* a *será denotado* $-a$*.)*

v. (Associatividade da multiplicação) *Para todo* a*,* b *e* $c \in A$*, temos* $(ab)c = a(bc)$*.*

vi. (Distributividade da multiplicação) *Para todo* a*,* b *e* $c \in A$*, temos* $a(b+c) = ab + ac$ *e* $(b + c)a = ba + ca$*.*

Observações:

1) A multiplicação não é, necessariamente, comutativa. Quando isso ocorrer A será denominado **anel comutativo**.

2) Um anel não necessita ter elemento neutro da multiplicação (chamado **unidade do anel** e denotado por 1). Caso isso ocorra, dizemos que A é um **anel com unidade**.

3) Os elementos de um anel A que possuem inverso multiplicativo são chamados **invertíveis** ou **unidades de** A (notação: $U(A) = \{x \in A \mid x \text{ é uma unidade de } A\}$). Note que não é necessário que os elementos de um anel tenham inversos multiplicativos.

É fácil ver que os conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $M_m(\mathbb{Z})$ (matrizes $m \times m$ com entradas inteiras) e $\mathbb{Z}[x]$ (polinômios na variável x com coeficientes inteiros) - com a soma e o produto usuais - satisfazem a definição acima. Portanto, representam alguns exemplos de anéis.

1.1.1 Domínios Integrais

Definição 1.1.2 *Um elemento não nulo a de um anel comutativo A é chamado* ***divisor de zero*** *se existe um elemento não nulo b em A tal que $ab = 0$.*

Definição 1.1.3 *Um anel comutativo com unidade é chamado* ***domínio integral*** *ou* ***domínio*** *se ele não possui divisor de zero.*

Exemplos:

1) O anel $\mathbb{Z}[x]$ é um domínio integral. Para demonstrar isso, suponha que $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$, em $\mathbb{Z}[x]$, sejam não nulos e que o produto $f(x) \cdot g(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$, onde $c_k = a_kb_0 + a_{k-1}b_1 + \cdots + a_0b_k$ com $0 \leq k \leq n+m$, seja nulo. Como $f(x)$ e $g(x)$ são não nulos, sejam i e j os menores índices tais que $a_i \neq 0$ e $b_j \neq 0$. Assim, $c_{i+j} = a_ib_j \neq 0$, donde $f(x) \cdot g(x) \neq 0$, o que é um absurdo. Logo, $f(x) \cdot g(x) = 0$ se $f(x)$ ou $g(x)$ é nulo.

2) O anel $M_2(\mathbb{Z})$ não é um domínio integral. Tomemos, por exemplo, as matrizes não nulas $\begin{bmatrix} 3 & 2 \\ 0 & 0 \end{bmatrix}$ e $\begin{bmatrix} 2 & 0 \\ -3 & 0 \end{bmatrix}$, em $M_2(\mathbb{Z})$, cujo produto é $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

1.1.2 Corpos

Definição 1.1.4 *Um anel comutativo com unidade é chamado* ***corpo*** *se todo elemento não nulo é invertível.*

Exemplos:

1) Os conjuntos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos.

2) Considere o conjunto $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$. Esse conjunto é um corpo, pois é um anel comutativo com unidade 1 e, para todo elemento não nulo $a + b\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$, temos $(a + b\sqrt{3})^{-1} = \frac{a}{a^2-3b^2} - \frac{b}{a^2-3b^2}\sqrt{3}$.

Observe que todo corpo é um domínio. De fato, dados a e b pertencentes a um corpo com $a \neq 0$ e $a \cdot b = 0$, podemos multiplicar ambos os lados da última expressão por a^{-1} obtendo $b = 0$.

Consideraremos com mais atenção o anel $\mathbb{Z}_n$, uma vez que seu emprego na criptografia é bastante significativo. Para isso, é necessário recordarmos os conceitos de **ideal** e **anel quociente**.

1.1.3 Ideais

Definição 1.1.5 *Um subconjunto I de um anel A é* ***subanel de*** *A se I também for um anel com as operações de A.*

Definição 1.1.6 *Um subanel I de A será chamado* ***ideal de*** *A se para todo $a \in A$ e todo $x \in I$ tivermos $xa \in I$ e $ax \in I$.*

Exemplos:

1) Todo anel A possui os subanéis $\{0\}$ e A como ideais.

2) Seja n um inteiro positivo, o conjunto dos múltiplos de n, $n\mathbb{Z} = \{0, \pm n, \pm 2n, ...\}$, é um ideal de $\mathbb{Z}$. Na realidade, podemos provar que todos os ideais de $\mathbb{Z}$ são da forma $n\mathbb{Z}$, para algum n.

3) Seja A um anel comutativo com unidade e $x \in A$. O conjunto $< x >= \{ax \mid a \in A\}$ é um ideal de A gerado por x. Observe que $< x >$ é o menor ideal de A que contém x.

1.1.4 Anéis Quocientes

A partir de um anel A e de um ideal I de A definiremos um novo anel, $\frac{A}{I}$, denominado **anel quociente**. Para isso, vamos estabelecer a seguinte relação de equivalência entre os elementos do anel A:

$$a \sim a_1 \Leftrightarrow a - a_1 \in I.$$

Com efeito, as propriedades reflexiva, simétrica e transitiva são satisfeitas:

i. $a \sim a$, pois $a - a = 0 \in I$.

ii. Se $a \sim a_1$ então $a_1 \sim a$, pois $a - a_1 \in I \Rightarrow a_1 - a = -(a - a_1) \in I$, porque I é um ideal.

iii. Se $a \sim a_1$ e $a_1 \sim a_2$ então $a \sim a_2$, pois como $a - a_1 \in I$ e $a_1 - a_2 \in I$, somando esses elementos, temos que $a - a_2 \in I$ pela definição de ideal.

Como sabemos, toda relação de equivalência determina uma partição em A, isso significa que A será a reunião disjunta das classes de equivalência:

$$A = \dot{\bigcup_{a \in A}} [a]$$

onde $[a] = \{a_1 \in A \mid a_1 \sim a\} = \{a_1 \in A \mid a_1 - a \in I\} = \{a_1 \in A \mid a_1 \in a + I\}$.

Usaremos as notações $a + I$ para representar a classe $[a]$ e

$$\frac{A}{I} = \{a + I \mid a \in A\}$$

para o conjunto das classes de equivalência de A, determinadas pela relação $\sim$.

Em $\frac{A}{I}$ podemos definir as operações:

$$(a+I)+(b+I)=(a+b)+I \quad \text{e} \quad (a+I)\cdot(b+I)=(a\cdot b)+I.$$

Para verificar que $(\frac{A}{I},+,\cdot)$ é um anel, observe que como $a+I$ e $b+I$ são classes, ou seja, conjuntos, é necessário que as operações acima estejam bem definidas. Isso quer dizer que essas operações não devem depender do representante da classe escolhido. Assim, se $a+I=a_1+I$ e $b+I=b_1+I$, então devemos ter $(a+b)+I=(a_1+b_1)+I$ e $(a\cdot b)+I=(a_1\cdot b_1)+I$.

Com efeito, como $(a+I)=(a_1+I)$ e $(b+I)=(b_1+I)$ então $(a-a_1)\in I$ e $(b-b_1)\in I$. Além disso, como I é um ideal $(a-a_1)+(b-b_1)\in I$, ou seja, $(a+b)-(a_1+b_1)\in I$. Dessa forma, pela definição da relação de equivalência, temos que $(a+b)\sim(a_1+b_1)$, donde $(a+b)+I=(a_1+b_1)+I$. Portanto, a soma está bem definida.

Temos ainda que, $ab-a_1b_1=ab-a_1b+a_1b-a_1b_1=(a-a_1)b+a_1(b-b_1)$. Como I é um ideal, $(a-a_1)b\in I$ e $a_1(b-b_1)\in I$, donde $ab-a_1b_1\in I$. Assim, $(ab)\sim(a_1b_1)$, ou seja, $(ab)+I=(a_1b_1)+I$. Portanto, o produto também está bem definido.

Estando as duas operações bem definidas, é fácil ver que $(\frac{A}{I},+,\cdot)$ é um anel com elemento neutro $0+I$ e com o inverso aditivo de $a+I$ igual a $-a+I$.

Exemplos:

1) Considere o anel $\mathbb{Z}$ e seu ideal $4\mathbb{Z}$. Assim, pela definição de anel quociente, $\frac{\mathbb{Z}}{4\mathbb{Z}}=\{0+4\mathbb{Z},1+4\mathbb{Z},2+4\mathbb{Z},3+4\mathbb{Z}\}$.

2) Seja $A=\{\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \mid a_i\in\mathbb{Z}\}$ e I subconjunto de A formado pelas matrizes com entradas pares, isto é, $I=\{\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \mid a_i\in 2\mathbb{Z}\}$. É fácil ver que I é ideal de A e que $\frac{A}{I}=\{\begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix}+I \mid r_i\in\{0,1\}\}$ é um anel não comutativo com unidade que possui 16 elementos. Para descobrir qual dos 16 elementos é, por exemplo, $\begin{bmatrix} 5 & -7 \\ 4 & 2 \end{bmatrix}+I$, basta observar que $\begin{bmatrix} 5 & -7 \\ 4 & 2 \end{bmatrix}+I=\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}+\begin{bmatrix} 4 & -8 \\ 4 & 2 \end{bmatrix}+I=\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}+I$, uma vez que um ideal absorve seus próprios elementos.

Em seguida, generalizaremos esses exemplos definindo o anel $\mathbb{Z}_n$ e o anel $M_m(\mathbb{Z}_n)$.

1.1.5 O anel $\mathbb{Z}_n$

Sendo n um inteiro positivo, sabemos que $n\mathbb{Z}$ é um ideal de $\mathbb{Z}$, esse fato nos permite definir o anel

$$\frac{\mathbb{Z}}{n\mathbb{Z}}=\{0+n\mathbb{Z},1+n\mathbb{Z},...,n-1+n\mathbb{Z}\},$$

com as operações:

$$(a+n\mathbb{Z})+(b+n\mathbb{Z})=(a+b)+n\mathbb{Z} \quad \text{e} \quad (a+n\mathbb{Z})\cdot(b+n\mathbb{Z})=(a\cdot b)+n\mathbb{Z}.$$

Esse anel é comutativo, pois $\mathbb{Z}$ o é, com unidade $1+n\mathbb{Z}$.

Com o objetivo de simplificarmos a notação, representaremos $\frac{\mathbb{Z}}{n\mathbb{Z}}$ por $\mathbb{Z}_n$ e $a+n\mathbb{Z}$ por $\overline{a}$, ou simplesmente a, quando o contexto deixar claro que estamos trabalhando com os elementos desse anel.

Dessa forma, o anel quociente $\frac{\mathbb{Z}}{n\mathbb{Z}}$ será denotado por

$$\mathbb{Z}_n=\{\overline{0},\overline{1},...,\overline{n-1}\}$$

com as operações:

$$\overline{a}+\overline{b}=\overline{a+b} \quad \text{e} \quad \overline{a}\cdot\overline{b}=\overline{a\cdot b}.$$

Nem todos elementos de $\mathbb{Z}_n$ possuem inverso multiplicativo. Por exemplo, em $\mathbb{Z}_4=\{\overline{0},\overline{1},\overline{2},\overline{3}\}$ não existe nenhuma classe $\overline{a}$ tal que $\overline{a}\cdot\overline{2}=\overline{1}$, isto é, $\nexists\ \overline{2}^{-1}$.

Proposição 1.1.1 *$\overline{a}\in\mathbb{Z}_n$ é invertível $\Leftrightarrow mdc(a,n)=1$.*

Demonstração:

Se $\overline{a}\in\mathbb{Z}_n$ é invertível, então $\exists\ \overline{r}\in\mathbb{Z}_n$ tal que $\overline{a}\cdot\overline{r}=1$. Dessa forma, $ar-1$ é múltiplo de n, donde $ar+ns=1$, para algum $s\in\mathbb{Z}$. Assim, $mdc(a,n)=1$.

Por outro lado, se $mdc(a,n)=1$, $\overline{a}\in\mathbb{Z}_n$, pelo algoritmo de Euclides, existem r e s tais que $ar+ns=1$. Usando classes de equivalência, temos que $\overline{ra}=\overline{1}$, donde $\overline{a}$ é invertível em $\mathbb{Z}_n$ com $\overline{a}^{-1}=\overline{r}$.

(Notação: O conjunto das unidades de $\mathbb{Z}_n$ será denotado $U(n)$.)

A seguir, apresentaremos um resultado que nos será muito útil.

Proposição 1.1.2 *$\mathbb{Z}_n$ é corpo $\Leftrightarrow$ n é primo.*

Demonstração:

Suponha, por absurdo, que $\mathbb{Z}_n$ é corpo e $n=xy$ com $x,y\in\mathbb{Z}$ tais que $0<x,y<n$. Dessa forma, $\overline{xy}=\overline{0}$ donde $\overline{x}=\overline{0}$ ou $\overline{y}=\overline{0}$, pois $\mathbb{Z}_n$ é corpo, isto é, domínio. Assim, $n\mid x$ ou $n\mid y$, o que é um absurdo. Logo n é primo.

Por outro lado, se n é primo, então $\forall\ \overline{a}\in\mathbb{Z}_n-\{\overline{0}\}$ temos que $mdc(n,a)=1$. Escrevendo 1 como combinação linear de n e a, obtemos $ax+ny=1$. Usando classes de equivalência, $\overline{ax+ny}=\overline{1}\Rightarrow\overline{ax}=\overline{1}$, donde $\overline{a}\ \overline{x}=\overline{1}$. Assim, $\overline{a}$ possui inverso, ou seja, $\mathbb{Z}_n$ é corpo.

1.1.6 Anel das matrizes $M_m(A)$

Vamos considerar também o conjunto $M_m(A)$ das matrizes $m\times m$ com entradas em um anel A comutativo com unidade. Nosso objetivo é mostrar que $M_m(A)$ é um anel com

unidade, e estabelecer a condição para que uma matriz desse conjunto seja invertível.

Uma matriz $A_{m\times n}$ com entradas em um anel A é uma tabela de mn elementos de A organizados em m linhas e n colunas:

$$A_{m\times n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix},$$

onde a_{ij} representa a entrada da linha i e coluna j de $A_{m\times n}$.

Observação:
Estaremos utilizando a notação A tanto para uma matriz $A_{m\times n}$ (ou A_m, quando se tratar de matriz quadrada), quanto para o anel A das entradas de tal matriz. Isso será feito sem prejuízo à compreensão do texto, uma vez que sempre deixaremos claro à qual estrutura estamos nos referindo. A notação $A_{m\times n}$ (ou A_m) será mantida apenas quando julgarmos necessário.

Podemos definir a soma de duas matrizes A e B, de ordem $m \times n$, como uma matriz C, $m \times n$, obtida a partir da soma dos elementos correspondentes de A e B, isto é,

$$c_{ij} = a_{ij} + b_{ij},$$

para i e j, tais que $1 \square i \square m$ e $1 \square j \square n$.

Em seguida, definiremos a multiplicação de uma matriz A por um escalar. Apesar de não usarmos essa operação na estrutura de anel, ela será utilizada para determinarmos a inversa de uma matriz.

A multiplicação de uma matriz A, $m \times n$, por um escalar α, é a matriz αA, $m \times n$, obtida multiplicando-se cada elemento da matriz A por α.

Além disso, quando temos duas matrizes $A_{m\times p}$ e $B_{p\times n}$ (o número de colunas da primeira é igual ao número de linhas da segunda) podemos definir a matriz $C_{m\times n} = AB$, tal que

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \cdots + a_{ip}b_{pj} = \sum_{k=1}^{p} a_{ik}b_{kj}$$

para i e j, tais que $1 \square i \square m$ e $1 \square j \square n$.

Agora que já definimos a soma, o produto por um escalar e o produto de matrizes, focalizaremos nossa atenção no conjunto $M_m(A)$ das matrizes quadradas de ordem m com entradas em um anel A comutativo com unidade.

Observe que se as matrizes A e B pertencem a $M_m(A)$, então $A + B$ e AB pertencem a $M_m(A)$, pois os resultados dessas operações também são matrizes $m \times m$ com entradas no anel A. Assim, $M_m(A)$ é fechado em relação à soma e à multiplicação.

Proposição 1.1.3 *Se A é um anel comutativo com unidade, então $M_m(A)$ é um anel com unidade.*

Demonstração:

Para provarmos que $M_m(A)$ é um anel, com as operações de soma e produto definidas acima, verificaremos as propriedades da definição 1.1.1.

A comutatividade e a associatividade da soma decorrem diretamente do fato de que A é um anel.

O elemento neutro da adição é a matriz $m \times m$ com todas as entradas nulas. Já o elemento simétrico de A_m é a matriz $-A_m$, cujas entradas são formadas pelos elementos simétricos das entradas de A_m.

Além disso, a multiplicação é associativa, pois dadas as matrizes A, B e $C \in M_m(A)$, temos que

$$[A(BC)]_{ij} = \sum_{k=1}^{n} a_{ik} [BC]_{kj} = \sum_{k=1}^{n} a_{ik}(\sum_{l=1}^{n} b_{kl}c_{lj}) = \sum_{k=1}^{n} \sum_{l=1}^{n} a_{ik}(b_{kl}c_{lj}) =$$

$$\sum_{k=1}^{n} \sum_{l=1}^{n} (a_{ik}b_{kl})c_{lj} = \sum_{l=1}^{n} \sum_{k=1}^{n} (a_{ik}b_{kl})c_{lj} = \sum_{l=1}^{n} (\sum_{k=1}^{n} a_{ik}b_{kl})c_{lj} =$$

$$\sum_{l=1}^{n} [AB]_{il} c_{lj} = [(AB)C]_{ij} ,$$

onde $[A(BC)]_{ij}$ representa a entrada da linha i e coluna j da matriz $A(BC)$; $[BC]_{kj}$ a entrada da linha k e coluna j da matriz BC; e assim por diante.

E, por último, para toda matriz A, B e $C \in M_m(A)$ temos $A(B + C) = AB + AC$ e $(B + C)A = BA + CA$. De fato,

$$[A(B + C)]_{ij} = \sum_{k=1}^{n} a_{ik} [B + C]_{kj} = \sum_{k=1}^{n} a_{ik}(b_{kj} + c_{kj}) = \sum_{k=1}^{n} (a_{ik}b_{kj} +$$

$$a_{ik}c_{kj}) = \sum_{k=1}^{n} a_{ik}b_{kj} + \sum_{k=1}^{n} a_{ik}c_{kj} = [AB]_{ij} + [AC]_{ij} = [AB + AC]_{ij}.$$

Analogamente, demonstra-se que $[(B + C)A]_{ij} = [BA + CA]_{ij}$.

Seja

$$I_m = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix},$$

é fácil ver que para toda matriz $A \in M_m(A)$, temos $AI_m = I_m A = A$. Logo, I_m é unidade de $M_m(A)$.

Portanto, $M_m(A)$ é um anel com unidade.

Veremos, no capítulo 3, uma aplicação do anel das matrizes na criptografia. Para que possamos entender o processo de cifragem e decifragem de mensagens utilizando esse recurso, será necessário estabelecer as condições sob as quais uma matriz do anel $M_m(A)$ é invertível. Tendo isso em mente, definiremos **determinante** e **matriz adjunta** de uma matriz A_m.

O **determinante de uma matriz** 1×1, $A = [a]$, é o próprio elemento a (notação:

$detA_1 = a$).

No caso de uma matriz 2×2, definimos o **determinante de** A da seguinte forma:

$$detA = det \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

Já para uma matriz 3×3, vamos primeiro relembrar a definição de **cofator do elemento** a_{ij}.

O **cofator do elemento** a_{ij} de uma matriz 3×3, denotado Δ_{ij}, é:

$$\Delta_{ij} = (-1)^{i+j} detA_{ij},$$

onde A_{ij} é a submatriz 2×2 da matriz inicial, onde retiramos a linha i e a coluna j.

Utilizando cofatores, o **determinante de uma matriz** 3×3 será definido por:

$$detA = det \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = a_{11}\Delta_{11} + a_{12}\Delta_{12} + a_{13}\Delta_{13}.$$

Aqui fixamos a primeira linha da matriz para desenvolvermos o determinante. Note que poderíamos ter tomado qualquer outra linha ou coluna, pois isso nos levaria ao mesmo resultado.

De modo análogo ao que fizemos para definir o determinante de uma matriz 3×3, podemos definir o **determinante de matrizes** $m \times m$ a partir do determinante de uma matriz $(m-1) \times (m-1)$. Assim, temos que

$$detA = a_{11}\Delta_{11} + a_{12}\Delta_{12} + \cdots + a_{1m}\Delta_{1m} = \sum_{j=1}^{m} a_{1j}\Delta_{1j}$$

(desenvolvimento em cofatores do determinante da matriz A, $m \times m$, em termos da primeira linha), onde

$$\Delta_{1j} = (-1)^{1+j} detA_{1j}.$$

Novamente poderíamos ter fixado qualquer linha ou coluna.

Proposição 1.1.4 *Se uma matriz A de ordem $m \times m$ possui duas linhas iguais, então $detA = 0$.*

Demonstração:

A demonstração será feita utilizando indução matemática sobre a ordem de A.

Se A é uma matriz 2×2, tal que $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{11} & a_{12} \end{bmatrix}$, então $detA = a_{11}a_{12} - a_{12}a_{11} = 0$.

Supondo essa proposição válida para matrizes de ordem $(m-1) \times (m-1)$, vamos provar que ela é válida para matrizes $m \times m$.

Seja A, uma matriz $m \times m$, tal que as linhas k e l $(k \neq l)$ sejam iguais. Desenvolvendo o $detA$ em termos de uma linha $i \neq k, l$, temos

$$detA = \sum_{j=1}^{m} a_{ij}(-1)^{i+j} detA_{ij},$$

onde A_{ij} é uma matriz $(m-1) \times (m-1)$ com duas linhas iguais. Assim, $detA_{ij} = 0 \Rightarrow detA = 0$.

Proposição 1.1.5 *Dadas as matrizes A e B, de ordem $m \times m$, temos que $det(AB) = (detA)(detB)$.*

Para não prolongarmos muito nossas discussões, omitiremos a demonstração dessa proposição. Os leitores interessados poderão encontrá-la em Santos [20].

Com os cofatores de uma matriz A, $m \times m$ podemos obter uma nova matriz $\overline{A}$, $m \times m$ chamada **matriz dos cofatores de** A:

$$\overline{A} = \begin{bmatrix} \Delta_{11} & \Delta_{12} & \cdots & \Delta_{1m} \\ \Delta_{21} & \Delta_{22} & \cdots & \Delta_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{m1} & \Delta_{m2} & \cdots & \Delta_{mm} \end{bmatrix}.$$

Denominamos **matriz adjunta de** A à transposta da matriz $\overline{A}$ dos cofatores de A:

$$adjA = \begin{bmatrix} \Delta_{11} & \Delta_{21} & \cdots & \Delta_{m1} \\ \Delta_{12} & \Delta_{22} & \cdots & \Delta_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{1m} & \Delta_{2m} & \cdots & \Delta_{mm} \end{bmatrix}.$$

Proposição 1.1.6 *Se A é uma matriz de ordem $m \times m$, então $A(adjA) = (detA)I_m$.*

Demonstração:

$$\text{Seja } C = A(adjA) = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{bmatrix} \begin{bmatrix} \Delta_{11} & \Delta_{21} & \cdots & \Delta_{m1} \\ \Delta_{12} & \Delta_{22} & \cdots & \Delta_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{1m} & \Delta_{2m} & \cdots & \Delta_{mm} \end{bmatrix} =$$

$$\begin{bmatrix} a_{11}\Delta_{11} + \cdots + a_{1m}\Delta_{1m} & a_{11}\Delta_{21} + \cdots + a_{1m}\Delta_{2m} & \cdots & a_{11}\Delta_{m1} + \cdots + a_{1m}\Delta_{mm} \\ a_{21}\Delta_{11} + \cdots + a_{2m}\Delta_{1m} & a_{21}\Delta_{21} + \cdots + a_{2m}\Delta_{2m} & \cdots & a_{21}\Delta_{m1} + \cdots + a_{2m}\Delta_{mm} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}\Delta_{11} + \cdots + a_{mm}\Delta_{1m} & a_{m1}\Delta_{21} + \cdots + a_{mm}\Delta_{2m} & \cdots & a_{m1}\Delta_{m1} + \cdots + a_{mm}\Delta_{mm} \end{bmatrix}.$$

Nessa matriz, temos que cada elemento da diagonal principal, c_{ii}, é igual ao determinante da matriz A desenvolvido em termos da linha i.

Por outro lado, cada elemento fora da diagonal principal, c_{ij} $(i \neq j)$, é o determinante

de uma matriz que possui duas linhas iguais. Por exemplo,

$$c_{12} = a_{11}\Delta_{21} + a_{12}\Delta_{22} + \cdots + a_{1m}\Delta_{2m} = det \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{11} & a_{12} & \cdots & a_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{bmatrix}.$$

Portanto, pela proposição 1.1.4, $c_{ij} = 0$, $\forall i \neq j$.

Assim,

$$C = A(adjA) = \begin{bmatrix} detA & 0 & \cdots & 0 \\ 0 & detA & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & detA \end{bmatrix} = (detA) \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} =$$

$(detA)I_m$.

Teorema 1.1.1 *Uma matriz $A \in M_m(A)$ é invertível $\Leftrightarrow$ $detA \in U(A)$.*

Demonstração:

Supondo $A \in M_m(A)$ invertível, temos que existe A^{-1}, tal que $AA^{-1} = I_m$. Usando a proposição 1.1.5, $det(AA^{-1}) = (detA)(detA^{-1}) = detI_m$. É fácil ver que $detI_m = 1$, dessa forma, $(detA)(detA^{-1}) = 1$. Donde $detA^{-1} = (detA)^{-1}$. Assim, $detA$ é uma unidade de A.

Por outro lado, pela proposição 1.1.6, $A(adjA) = (detA)I_m$. Se $detA_m \in U(A)$, então $A(detA_m)^{-1}(adjA_m) = I_m$. Assim, A é invertível com $A^{-1} = (detA)^{-1}(adjA)$. Observe que estamos usando a propriedade $\alpha(AB) = A(\alpha B)$, cuja demonstração pode ser encontrada em Santos [20].

Assim, $U(M_m(A)) = \{B \in M_m(A) \mid detB \in U(A)\}$.

1.1.7 O anel $M_m(\mathbb{Z}_n)$

Pela proposição 1.1.3, o conjunto $M_m(\mathbb{Z}_n)$ das matrizes $m \times m$ com entradas no anel $\mathbb{Z}_n$, com a soma e a multiplicação definidas na seção anterior, é um anel com unidade, pois $\mathbb{Z}_n$ é comutativo com unidade.

Além disso, a partir do teorema 1.1.1 e da proposição 1.1.1, concluímos que uma matriz $A \in M_m(\mathbb{Z}_n)$ é invertível $\Leftrightarrow$ $mdc(d, n) = 1$, onde $\overline{d} = detA$.

Exemplos:

1) A matriz $A = \begin{bmatrix} 25 & 12 \\ 17 & 14 \end{bmatrix} \in M_2(\mathbb{Z}_{26})$ não é invertível. De fato, $\overline{d} = detA = 16$, donde $mdc(d, n) \neq 1$, isto é, $detA \notin U(26)$.

2) Uma matriz invertível em $M_3(\mathbb{Z}_{26})$ é $B = \begin{bmatrix} 2 & 17 & 19 \\ 3 & 4 & 7 \\ 0 & 1 & 2 \end{bmatrix}$, pois $detB = 9 \in U(26)$.

Como vimos na demonstração do teorema 1.1.1, sua inversa, $B^{-1} = \begin{bmatrix} 3 & 7 & 25 \\ 8 & 12 & 25 \\ 9 & 20 & 1 \end{bmatrix}$, pode ser obtida calculando $(detB)^{-1} \cdot (adjB)$.

1.2 Grupos

Definição 1.2.1 *Um **grupo** G é um conjunto com uma operação $*$ que satisfaz as seguintes condições:*

i. (Associatividade) *Para todo a, b e $c \in G$, temos $(a * b) * c = a * (b * c)$.*

ii. (Elemento neutro) *Para todo $a \in G$, existe um elemento e em G, tal que $a * e = e * a = a$.*

iii. (Elemento inverso) *Para cada $a \in G$, existe um elemento $b \in G$, tal que $a * b = b * a = e$.*

Observação:

Se para todo a e $b \in G$, tivermos $a * b = b * a$, então G será chamado **grupo abeliano**.

Exemplos:

1) Os anéis $\mathbb{Z}, \mathbb{R}, \mathbb{C}$ e $\mathbb{Z}_n$ são grupos aditivos com elemento neutro 0 e com o inverso de a igual a $-a$. De forma geral, todo anel é um grupo aditivo abeliano.

2) O conjunto $GL(2, \mathbb{R}) = \{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \mid a_i \in \mathbb{R}, a_1a_4 - a_2a_3 \neq 0\}$ das matrizes 2×2 com entradas reais e determinante não nulo, é um grupo multiplicativo com o produto usual.

3) Para $n = 12$ temos $U(12) = \{1, 5, 7, 11\}$ (unidades de $\mathbb{Z}_{12}$). Esse conjunto forma um grupo multiplicativo abeliano. Observe a tabela 1.1 que ilustra a multiplicação:

Tabela 1.1: Multiplicação dos elementos de $U(12)$.

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

É fácil ver que, no geral, o conjunto $U(A)$ - unidades de um anel A - é um grupo multiplicativo.

Definição 1.2.2 *A **ordem de um grupo** G é o número de elementos de G quando G for finito. (Notação: $|G|$.)*

Exemplos:

1) A ordem do grupo aditivo $\mathbb{Z}_n$ é $|(\mathbb{Z}_n, +)| = n$.

2) No exemplo 3 acima, temos que $|U(12)| = 4$.

Definição 1.2.3 *A **ordem de um elemento** a em um grupo G é o menor inteiro positivo n tal que $a^n = e$. Caso esse inteiro não exista, dizemos que a possui ordem infinita. (Notação: $|a|$.)*

Podemos demonstrar que $U(n) = \{\overline{a} \in \mathbb{Z}_n \mid mdc(a, n) = 1\}$ é um grupo multiplicativo com $|U(n)| = \Phi(n)$ (função de Euler) elementos, onde

$$\Phi(n) = p_1^{e_1-1}(p_1 - 1) \cdot ... \cdot p_k^{e_k-1}(p_k - 1),$$

se $n = p_1^{e_1} \cdot ... \cdot p_k^{e_k}$.

Dessa forma, se p é primo $U(p) = \mathbb{Z}_p - \{0\}$ é um grupo multiplicativo com $\Phi(p) = (p - 1)$ elementos.

Assim como definimos subanel de um anel A, podemos também definir subgrupo de um grupo G.

Definição 1.2.4 *Um subconjunto H de um grupo G é **subgrupo de** G se H também for um grupo com a operação de G.*

Exemplo:
O subconjunto $\{0, 2, 4, 6, 8, 10\}$ do grupo aditivo $\mathbb{Z}_{12}$ é um subgrupo de $\mathbb{Z}_{12}$, pois satisfaz as propriedades que definem um grupo.

Em seguida, enunciaremos e demonstraremos um dos mais importantes teoremas da teoria dos grupos finitos.

1.2.1 Teorema de Lagrange e algumas conseqüências

Teorema 1.2.1 *Se G é um grupo finito e H é um subgrupo de G, então $|H|$ divide $|G|$.*

Demonstração:
Para demonstrarmos o Teorema de Lagrange, vamos definir a seguinte relação de equivalência em G:

$$a \sim a_1 \Leftrightarrow aa_1^{-1} \in H.$$

Com efeito, as propriedades reflexiva, simétrica e transitiva são satisfeitas:

i. $a \sim a$, pois $aa^{-1} = e \in H$.

ii. Se $a \sim a_1$ então $a_1 \sim a$, pois $aa_1^{-1} \in H \Rightarrow a_1a^{-1} = (aa_1^{-1})^{-1} \in H$, porque H é um subgrupo.

iii. Se $a \sim a_1$ e $a_1 \sim a_2$ então $a \sim a_2$, pois como $aa_1^{-1} \in H$ e $a_1a_2^{-1} \in H$, temos $aa_1^{-1}a_1a_2^{-1} = aa_2^{-1} \in H$.

Dessa forma, como $\sim$ determina uma partição em G, temos que

$$G = \dot{\bigcup_{a \in G}} [a]$$

onde $[a] = \{a_1 \in G \mid a_1 \sim a\} = \{a_1 \in G \mid a_1 a^{-1} \in H\} = \{a_1 \in G \mid a_1 \in Ha\}$.

Usaremos a notação Ha (classe lateral à direita de H) para a classe $[a]$.

Todas as classes de equivalência de G, determinadas pela relação $\sim$, possuem o mesmo número de elementos. Isso é verdade uma vez que existe uma bijeção entre uma classe qualquer e o subgrupo H:

$$\begin{aligned} f : Ha &\to H \\ ha &\longmapsto h. \end{aligned}$$

De fato, f é injetiva, pois $f(h_1 a) = f(h_2 a)$, significa que $h_1 = h_2$, donde $h_1 a = h_2 a$. Além disso, dado qualquer $h \in H$, existe $h_1 a \in Ha$, tal que $f(h_1 a) = h$, basta tomar $h_1 a = ha$. Portanto, f é sobrejetiva.

Como todas as classes de G possuem a mesma quantidade de elementos, temos que $|G| = r|H|$, onde r representa o número de classes de equivalência de G em relação a H. Logo, $|H|$ divide $|G|$.

Corolário 1.2.1 *Se G é um grupo finito e $a \in G$, então $a^{|G|} = e$.*

Demonstração:

É fácil ver que se G é um grupo e a é um elemento de G, então o subconjunto de G, gerado por a, $< a >= \{a^1, a^2, ..., e\}$ é um subgrupo de G. Dessa forma, pelo Teorema de Lagrange, $|< a >|$ divide $|G|$, ou seja, $|G| = |< a >| \; q$. Assim, $a^{|G|} = a^{|<a>|q}$, como $|a| = |< a >|$ temos que $a^{|<a>|q} = a^{|a|q} = e^q = e$.

Corolário 1.2.2 ***(Teorema de Euler)*** *Se n é um inteiro positivo e a é um inteiro tal que $mdc(a, n) = 1$, então $a^{\Phi(n)} = 1$ em $\mathbb{Z}_n$.*

Demonstração:

Como $mdc(a, n) = 1$, temos que $a \in U(n)$. Dessa forma, como $\mid U(n) \mid = \Phi(n)$, pelo corolário 1.2.1, $a^{\Phi(n)} = 1$ em $\mathbb{Z}_n$.

Corolário 1.2.3 ***(Pequeno teorema de Fermat)*** *Se p é um primo e a é um inteiro não divisível por p, então $\overline{a}^{p-1} = \overline{1}$ em $\mathbb{Z}_p$.*

Demonstração:

Sejam $a \in \mathbb{Z}$ e p, um primo, tal que p não divide a. Dessa forma, $mdc(a, p) = 1$, donde $\overline{a} \in U(p)$. Como $\mid U(p) \mid = \Phi(p) = p - 1$, pelo corolário 1.2.1, temos que $\overline{a}^{p-1} = \overline{1}$ em $\mathbb{Z}_p$.

Capítulo 2

Criptografia: evolução e importância do seu uso

A **criptografia** - do grego: *kryptos* (escondido, oculto) e *grapho* (grafia, escrita) - surgiu a partir da necessidade de manter o sigilo das comunicações à distância, protegendo-as contra a ação de espiões.

Essa ciência consiste de um conjunto de métodos que permitem codificar um texto, tornando-o ininteligível, de modo que apenas seu destinatário legítimo consiga decodificá-lo.

Para que possamos entender os processos de codificação e decodificação de mensagens, é necessário definirmos alguns termos.

Uma **mensagem original** é o texto que queremos enviar, e o texto codificado é chamado **mensagem cifrada**.

O processo de converter a mensagem original em mensagem cifrada é conhecido como **cifrar** ou **criptografar**. O de recuperar a mensagem original a partir da mensagem cifrada é chamado de **decifrar**.

Os métodos usados para cifrar e decifrar uma mensagem constituem um **sistema criptográfico** (ou **cripto-sistema**). Algumas vezes, também denominamos um sistema criptográfico simplesmente de cifra. Em geral, usamos em cada sistema criptográfico números que chamamos de **chaves**, para cifrar e decifrar mensagens. Quando a chave de deciframento é igual à chave de ciframento, ou é facilmente obtida a partir dessa, o cripto-sistema é denominado **cripto-sistema de chave secreta**. Caso contrário ele é chamado **cripto-sistema de chave pública**. A figura 2.1 esquematiza um sistema criptográfico.

Técnicas usadas para decifrar mensagens sem qualquer conhecimento da chave de deciframento, constituem a área de **criptoanálise**. Quando isso ocorre dizemos que houve **"quebra do código"**. As áreas de criptografia e criptoanálise constituem a **criptologia**.

Espera-se que o cripto-sistema seja suficientemente seguro para evitar que um oponente decifre a mensagem mesmo que conheça as operações de ciframento e deciframento. Para isso é necessário, entre outras coisas, que o sistema criptográfico possua um número significativo de chaves, evitando, dessa forma, que a mensagem seja revelada a partir da aplicação da operação de deciframento com as possíveis chaves.

Nos próximos capítulos, estudaremos sistemas criptográficos de chave secreta e de

chave pública, os quais usam principalmente a álgebra. Por ora apresentaremos uma síntese dos principais fatos ligados à evolução da criptografia, assim como destacaremos a importância do seu uso na proteção de informações sigilosas.

Figura 2.1: Esquema de um sistema criptográfico.

2.1 A evolução da criptografia

Como dissemos, a criptografia surgiu a partir da necessidade de manter o sigilo das comunicações à distância. Entretanto, a ameaça de interceptação de mensagens por espiões motivou não apenas o desenvolvimento de métodos para torná-las ininteligíveis, mas também o aparecimento de técnicas para ocultá-las.

Segundo Singh [23], o famoso historiador Heródoto foi responsável por alguns dos primeiros relatos nos quais a comunicação secreta esteve presente. Heródoto narrou, por exemplo, que Histaeu queria encorajar Aristágora de Mileto a se revoltar contra o rei persa. Para comunicar seus planos com segurança, Histaeu raspou a cabeça do mensageiro, escreveu a mensagem no seu couro cabeludo e esperou que seu cabelo crescesse novamente. O mensageiro então viajou e, chegando ao seu destino, raspou a cabeça revelando a mensagem para Aristágora.

A forma utilizada por Histaeu para esconder a mensagem é um exemplo de **esteganografia** - do grego: *steganos* (coberto) e *grapho* (grafia, escrita). A esteganografia abrange todos os métodos de comunicação secreta baseados na ocultação da mensagem.

Várias formas de esteganografia foram utilizadas durante muitos séculos. Entre os exemplos citados por Singh [23] podemos destacar também: a escrita de uma mensagem secreta em um pedaço de seda fina, que era amassada formando uma pequena bola, coberta com cera e engolida pelo mensageiro; e a escrita com tinta invisível, que com um leve aquecimento tornava-se marrom.

A criptografia se desenvolveu paralelamente à esteganografia, representando uma forma alternativa de comunicação secreta. O objetivo dos sistemas criptográficos não é esconder a existência de uma mensagem, mas evitar que uma pessoa desautorizada compreenda o seu significado, mesmo que tenha acesso às informações cifradas.

Os métodos que permitem cifrar mensagens podem ser classificados como: transposições, substituições ou cifra mentos compostos.

As **transposições** simplesmente permutam as letras de uma mensagem, de acordo com um padrão e uma chave previamente combinados entre o remetente e o destinatário.

Nas **substituições** as letras da mensagem original são trocadas por outras. A substituição é denominada **monoalfabética** quando não depende da posição da letra na mensagem, isto é, cada letra do texto original é representada em qualquer posição pela mesma substituta. Por outro lado, a substituição é chamada **polialfabética** quando depende da letra original e da sua posição no texto.

Nesse momento, não podemos deixar de citar um cripto-sistema de substituição monoalfabética bastante antigo denominado "cifra de deslocamento de César" ou "cifra de César". Esse cripto-sistema foi utilizado por Júlio César, imperador de Roma, para comunicar planos de batalha aos seus generais.

Na cifra de César, o ciframento de uma mensagem é feito substituindo-se cada letra por outra três posições à frente no alfabeto, como mostra a tabela 2.1.

Tabela 2.1: Correspondência de letras para a cifra de César.

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
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

Por último, podemos ainda ter cifra mentos compostos, os quais se fundamentam nos princípios da transposição e substituição simultaneamente.

Posteriormente, apresentaremos alguns cripto-sistemas de transposição, os principais sistemas de substituição, bem como um ciframento composto - o DES (Data Encryption Standard).

É interessante mencionar que assim como algumas formas de esteganografia, técnicas de transposição e substituição criptográfica já eram usadas desde o século V a.C. Algumas vezes, combinava-se métodos de criptografia e esteganografia aumentando significativamente a segurança da comunicação.

Cripto-sistemas de substituição monoalfabéticas, como a cifra de César, predominaram entre as formas de escrita secreta por vários séculos. Isso por que eram simples e ofereciam uma segurança considerável para a época.

Acreditava-se que um espião só conseguiria decifrar uma mensagem criptografada através de uma substituição monoalfabética, caso verificasse todas as substituições possíveis para as letras. Isso era considerado praticamente impossível, pois demandaria muito tempo (note que são 26! possibilidades de tabelas para um alfabeto de 26 letras). Dessa forma, os criadores de códigos se sentiam seguros e, conseqüentemente, nenhum desen-

volvimento notável ocorreu na criptografia no primeiro milênio.

De acordo com Singh [23], os árabes utilizaram substituições monoalfabéticas de maneira significativa. Além disso, na segunda metade do primeiro milênio, seus estudos possibilitaram o surgimento da criptoanálise. Como dissemos, essa ciência é constituída de técnicas que permitem decifrar mensagens sem o conhecimento da chave.

O "atalho" encontrado pelos árabes para decifrar mensagens criptografadas no sistema de substituição monoalfabética, consiste em comparar a freqüência das letras na mensagem à freqüência relativa das letras do alfabeto, no idioma da mensagem original. Porém, essa descoberta não se propagou rapidamente pelo mundo.

Segundo Singh [23], o uso da criptografia cresceu significativamente na Europa por volta do século XV. Mas, enquanto os intelectuais se familiarizavam com os métodos criptográficos, a criptoanálise começava a se desenvolver. Não se sabe se esse desenvolvimento ocorreu de forma independente na Europa ou se foi influenciado pelos árabes. De qualquer forma, alguns criptoanalistas europeus se destacaram por suas habilidades, entre eles, podemos citar nomes como: Giovanni Soro, Philibert Babou e François Viète.

Para Singh [23], esse foi, sem dúvida, um período de transição onde os criptógrafos ainda dependiam das cifras de substituição monoalfabéticas, enquanto os criptoanalistas começavam usar a análise de freqüência para quebrá-las.

Algumas estratégias começaram a ser utilizadas para melhorar o desempenho das cifras monoalfabéticas. Os criptógrafos começaram a tomar medidas como escrever as palavras com a grafia errada antes da codificação, para dificultar a análise de freqüência, ou ainda, introduzir símbolos secretos para algumas palavras. Porém, tais medidas não representaram obstáculo algum diante do poder dos criptoanalistas.

Um episódio que ilustra bem essa fase da criptografia é narrado por Singh [23]. Segundo ele, em 1586, Maria, rainha da Escócia, foi acusada de ajudar planejar a morte da sua prima Elizabeth, rainha da Inglaterra, e julgada por traição. Caso Maria fosse considerada realmente culpada, seria condenada à morte.

Por outro lado, a rainha Elizabeth tinha alguns motivos para não querer executar Maria. Entre eles, o receio de criar precedentes para que os rebeldes também a matassem. Assim, Elizabeth declarou que só concordaria em condenar Maria se houvesse uma prova concreta da sua participação.

Singh [23] conta, que após muitos anos de reinado, as coisas não iam bem para Maria na Escócia. Várias circunstâncias fizeram com que ela seguisse para a Inglaterra, na esperança de que sua prima, Elizabeth, fosse lhe ajudar. Porém, para Elizabeth, Maria representava uma ameaça. Elizabeth era uma rainha protestante e os conspiradores católicos almejavam que o trono fosse ocupado pela rainha Maria, também católica. Assim, ao procurar refúgio na corte inglesa, Maria encontrou uma prisão imposta por Elizabeth.

Maria ficou aprisionada em diversos castelos e a cada ano perdia parte dos poucos direitos que tinha. Ela foi privada até mesmo de receber e enviar correspondências. Enfim, haviam vários motivos para que desejasse a morte de Elizabeth.

Quando as esperanças de Maria estavam acabando, ela recebeu um pacote com correspondências contrabandeadas por um católico inglês. Daí em diante, ele começou a atuar como mensageiro levando mensagens para Maria e enviando suas mensagens. Tudo era feito de forma secreta: as mensagens eram escondidas em sacos de couro, e colocadas em

tampas ocas de barris de cerveja que eram levados para Maria. Por outro lado, Maria escondia mensagens nas tampas de barris vazios que eram retirados do castelo. Dessa maneira, ficou estabelecida uma comunicação razoavelmente segura entre Maria e seus simpatizantes. Assim, as relações entre ela e os conspiradores ingleses começaram a se estreitar.

Através dessas correspondências, Maria ficou sabendo que um plano para salvá-la estava sendo elaborado em Londres por Anthony Babington, um rapaz que tinha uma grande mágoa contra o governo que perseguira sua religião. Então ela resolveu enviar-lhe uma carta, através do mensageiro, na tentativa de conhecê-lo melhor, bem como seus planos.

Juntamente com seus amigos, Babington planejava assassinar a rainha Elizabeth para que a rainha Maria ocupasse o trono. Ao receber a carta de Maria, Babington escreveu seus planos de forma bem detalhada. E, mesmo sabendo que a carta chegaria à ela escondida - note que ao colocar as mensagens na tampa oca do barril de cerveja, o mensageiro usava uma forma de esteganografia -, tomou o cuidado extra de cifrá-la. Usou para isso, 23 símbolos para as letras do alfabeto, 35 símbolos para palavras mais comuns, 4 nulos e 1 símbolo para representar letras duplas conforme mostra a figura 2.2.

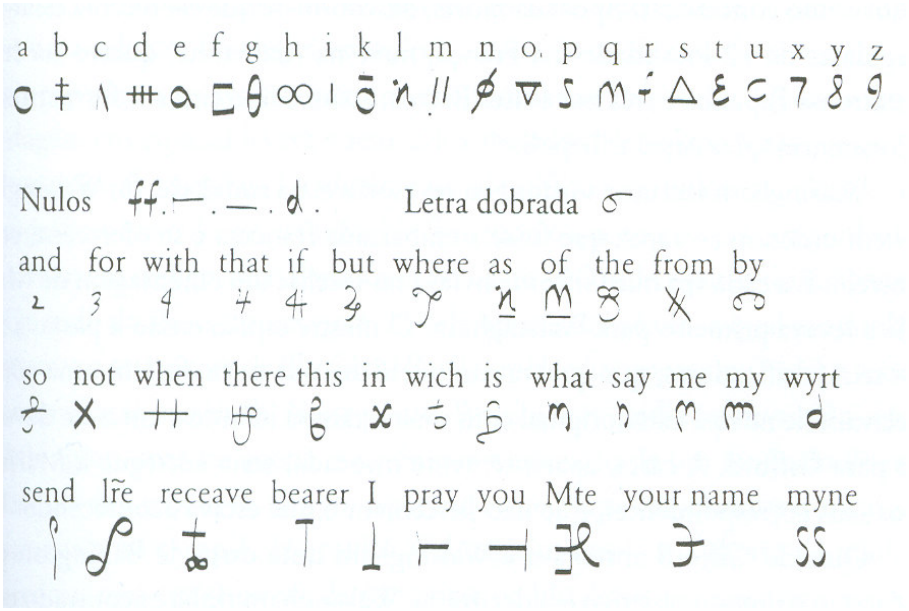

Figura 2.2: Cifra de Maria.

Utilizando essa cifra, várias outras correspondências foram trocadas entre Maria e Babington. Mas o que eles não sabiam é que o mensageiro não era totalmente confiável. Na verdade, ele tinha oferecido seu serviço como espião para o primeiro secretário da rainha Elizabeth, Sir Francis Walsingham.

Walsingham também era chefe da espionagem inglesa e conhecia um dos melhores criptoanalistas do país. Tal criptoanalista era especialista em análise de freqüência, além disso, conseguia identificar rapidamente os nulos e deduzia o significado das palavras em código a partir do contexto. Assim, com pouco esforço, ele teve acesso às informações sigilosas contidas nas correspondências de Maria e Babington.

Singh [23] encerra esse episódio relatando que, em seu julgamento, Maria tinha esperança de conseguir escapar da condenação à morte. Ela acreditava que mesmo que suas mensagens tivessem sido interceptadas, não seriam decifradas, pois tudo havia sido crip-

tografado. Mas, como dissemos, tudo havia sido decifrado e existiam provas suficientes para considerá-la culpada.

Maria realmente foi condenada e, em fevereiro de 1587, executada.

Diante do poder da criptoanálise em relação às cifras existentes, os criptógrafos sentiram necessidade de criar uma cifra mais forte. Ao final do século XVI Blaise Vigenère desenvolveu a idéia de outros cientistas, criando um novo sistema de codificação. Esse novo sistema, muito mais complexo que a cifra de substituição monoalfabética, foi denominado "cifra de Vigenère".

Ao contrário da cifra de César, que emprega o deslocamento de três posições no alfabeto para todas as letras da mensagem original, a cifra de Vigenère faz uso de deslocamentos diferentes, de acordo com a posição de cada letra na mensagem.

Como veremos no capítulo 3, o ciframento de uma mensagem é feito utilizando-se como chave uma seqüência de letras. Tal seqüência é associada às letras da mensagem e, com a correspondência entre letras e números dada abaixo na tabela 2.2, determina o deslocamento que cada letra da mensagem original sofrerá.

Tabela 2.2: Correspondência entre letras e números.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Quando a seqüência de letras utilizada tem tamanho menor que o do texto - usualmente uma palavra - ela deve ser repetida, quantas vezes for necessário, para que cada letra da mensagem fique associada a uma letra da chave.

Em particular, se considerarmos chaves formadas por uma única letra, a cifra de Vigenère pode ser vista como uma generalização de cifra de César. Por outro lado, se usarmos como chaves seqüências aleatórias de letras, de tamanho igual ao do texto, estaremos trabalhando com as chamadas "cifras one-time pad".

A cifra de Vigenère é um exemplo de substituição polialfabética. Como dissemos anteriormente, esse tipo de substituição não depende apenas da letra da mensagem original, mas também da sua posição no texto. Assim, letras iguais podem ser codificadas com substituições diferentes. Esse fato sugere a existência de uma grande vantagem da cifra de Vigenère em relação às cifras de substituição monoalfabéticas: a sua "imunidade" à análise de freqüência.

De acordo com Singh [23], apesar de representar uma cifra eficaz, a cifra de Vigenère só começou a ser usada alguns séculos após o seu desenvolvimento. Essa resistência dos criptógrafos em adotá-la é atribuída à sua falta de praticidade.

Nesse sentido, ainda surgiram algumas cifras na tentativa de melhorar o desempenho das cifras monoalfabéticas. Entre elas, a cifra de substituição homofônica, na qual as letras mais freqüentes são substituídas por mais de um símbolo, equilibrando-se a freqüência no texto cifrado.

Porém, os reforços para as cifras monoalfabéticas não foram suficientes por muito tem-

po. No século XVIII, havia uma preocupação dos governos europeus em formar centros de decifração de mensagens. Tais centros foram estabelecidos nas potências européias e denominados "Câmaras Negras".

Para as Câmaras Negras eram desviadas as correspondências codificadas. Tais correspondências eram facilmente decifradas nas mãos de profissionais como lingüistas, matemáticos, etc.

Com o desenvolvimento do telégrafo no século XIX e a introdução do código Morse (que não é uma forma de criptografia, apenas uma forma de representar letras e números por traços e pontos, para facilitar a transmissão de mensagens), um grande fluxo de mensagens importantes começou a ser enviado. Novamente, houve a necessidade de uma cifra forte, uma vez que as mensagens passavam antes pelas mãos dos telegrafistas. Dessa forma, a cifra de Vigenère finalmente foi adotada.

Ainda no século XIX, Charles Babbage, um gênio britânico, desenvolveu um método para decifrar mensagens codificadas pela cifra de Vigenère, quando essa utilizava chaves menores que o texto. No capítulo 3 ilustraremos tal método.

No final do século XIX, o italiano Guglielmo Marconi inventou o rádio. Essa invenção representou um grande avanço em relação ao telégrafo, pois não exigia a instalação de fios. O rádio facilitou a transmissão e a interceptação de mensagens e, com isso, intensificou a necessidade de desenvolvimento de cifras fortes. Mas até mesmo com a eclosão da 1ª Guerra Mundial as cifras continuaram sendo apenas adaptações e combinações de cifras que já haviam sido quebradas.

O famoso telegrama enviado por Arthur Zimmermann - ministro das Relações Exteriores da Alemanha - ao presidente mexicano, mostra a fragilidade das cifras da época. Esse telegrama continha informações diplomáticas extremamente sigilosas, propunha uma aliança contra os EUA na 1ª Guerra Mundial. Mas apesar de ter sido codificado com uma das cifras mais fortes da época, ele acabou sendo interceptado e decifrado pelos ingleses.

Mesmo após a 1ª Guerra Mundial a vantagem continuava sendo dos criptoanalistas. A única cifra realmente inquebrável, dentre todas que foram desenvolvidas, era a cifra one-time pad (cifra de Vigenère utilizando como chave de uma seqüência de letras aleatórias de tamanho igual ao do texto). Porém, quando o fluxo de mensagens não é pequeno, a produção e a distribuição de chaves para sua utilização é inviável.

Lester S. Hill introduziu em 1929 a "cifra de Hill", um outro cripto-sistema de substituição polialfabética, baseado em transformações matriciais. Porém, a segurança oferecida por essa cifra não era grande. Um método para quebrá-la foi rapidamente desenvolvido. Apesar disso, essa cifra será também considerada no próximo capítulo, uma vez que representa uma aplicação de alguns conceitos da álgebra e álgebra linear.

Segundo Singh [23], o avanço seguinte da criptografia, teve suas origens no século XV com o surgimento das primeiras máquinas criptográficas. Inicialmente essas máquinas eram constituídas por discos simples que mecanizavam as cifras de César e Vigenère como o mostrado na figura 2.3.

Figura 2.3: Disco de cifra utilizado na Guerra Civil americana.

No século XX o inventor alemão Arthur Scherbius aperfeiçoou a idéia trazida por esses discos. Com isso, deu origem a uma máquina criptográfica, bem mais complexa, denominada Enigma alemã. A figura 2.4 mostra uma máquina Enigma.

Inicialmente, a Enigma era constituída por: um teclado (para permitir a entrada das letras); três misturadores (responsáveis pela codificação das letras através de suas fiações internas); um painel de lâmpadas (com a função de indicar a letra codificada com sua iluminação); e um refletor (para possibilitar a obtenção da mensagem original, ao entrarmos com as letras da mensagem codificada, utilizando os ajustes iniciais da codificação.

Em uma versão posterior, Scherbius acrescentou mais uma peça, um painel de tomadas (para trocar o percurso de seis pares de letras); bem como possibilitou a remoção dos misturadores. Com isso, aumentou o número de chaves de 26^3 (orientações iniciais dos misturadores) para aproximadamente 10^{16} (disposição dos cabos no painel de tomadas, ordem dos misturadores e suas orientações iniciais).

Uma descrição detalhada do funcionamento da Enigma pode ser encontrada em Singh [23].

A invenção de Scherbius foi utilizada na Alemanha, durante vários anos, pelo governo, pelas empresas estatais e, principalmente, pelos militares. Com o início da 2ª Guerra Mundial os militares intensificaram ainda mais o seu uso. Assim foi possível proteger as comunicações com um alto nível de segurança.

A Enigma era extremamente forte e, por aproximadamente treze anos, os criptoanalistas franceses e britânicos acreditaram que mensagens cifradas por ela eram indecifráveis sem o conhecimento da chave. Até que após um árduo trabalho, o criptoanalista indiano Alan Turing conseguiu quebrá-la, na primeira metade da década de 40. Isso foi feito em Bletchley Park, onde ficava a sede da Escola de Cifras e Códigos do Governo (GC&CS) da Inglaterra, a partir do desenvolvimento das idéias de criptoanalistas poloneses.

Para quebrar o código produzido pela Enigma, Alan Turing desenvolveu máquinas

denominadas bombas. Tais máquinas foram capazes de identificar as chaves diárias utilizadas pelos militares alemães no decorrer da 2ª Guerra, através de um processo bastante complexo. Com isso, Alan Turing pôde decifrar as mensagens enviadas pelos alemães da mesma forma que os seus receptores legítimos. Esse fato contribuiu significativamente para a vitória dos aliados na 2ª Guerra Mundial.

Figura 2.4: A Enigma alemã.

Segundo Singh [23], paralelamente ao uso da Enigma pelos alemães, os americanos utilizaram outras alternativas de comunicação secreta. Entre elas, destacamos o uso de um idioma pouco conhecido, falado por uma tribo de índios americanos. Essa estratégia agilizou bastante a comunicação militar americana no decorrer da 2ª Guerra Mundial.

Além das bombas, um outro aparelho decifrador foi desenvolvido na Inglaterra, "o Colossus", com base nas idéias de Turing. Esse aparelho foi utilizado para decifrar as codificações feitas pela máquina Lorenz, empregada nas comunicações entre Hitler e seus generais.

De acordo com Singh [23], o Colossus apresentou duas vantagens em relação às bombas. A primeira delas é que ele era constituído de válvulas eletrônicas, bem mais rápidas que os antigos relés eletromecânicos utilizados nas bombas. A segunda é o fato de ser programável, característica que fez com que ele seja considerado o precursor do computador moderno. Dessa forma, dizemos que o computador teve sua origem na criptoanálise.

Apesar disso, com o passar do tempo, os criptógrafos contra-atacaram explorando o seu poder. Assim, foi possível criar cifras incorporando algoritmos mais complexos, o que fez com que a criptografia voltasse a prosperar.

Nos computadores, a codificação também se baseia nos princípios de substituição e transposição. Porém eles trabalham com números binários ao invés de letras e algarismos decimais. Para que isso seja possível, existem alguns protocolos como o ASCII (Código Padrão Americano para Troca de Informações), que utiliza sete dígitos para cada letra do alfabeto. A tabela 2.3 mostra a correspondência entre letras maiúsculas e números binários em ASCII.

Tabela 2.3: Correspondência entre letras maiúsculas e números binários em ASCII.

A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1011000
L	1001100	Y	1011001
M	1001101	Z	1011010

O uso da criptografia computacional também ficou sob controle governamental. Foram criados grandes centros como a Agência Nacional de Segurança (NSA - National Security Agency) nos EUA e o Quartel-General de Comunicações do Governo (GCHQ - Government Communications Headquarters) na Inglaterra reunindo alta tecnologia e mentes brilhantes. Essas organizações são responsáveis, entre outras coisas, pela escuta e análise de comunicações estrangeiras; assim como pela pesquisa de novas cifras para a proteção de comunicações governamentais e militares.

A princípio apenas o governo e os militares fizeram uso da criptografia computacional. Contudo, à medida em que os computadores foram se tornando mais baratos, o seu uso foi se difundindo entre as empresas para cifrar comunicações comerciais e financeiras.

Como cada empresa começou a usar um sistema particular para criptografar dados, apareceram dificuldades para a troca de mensagens secretas entre elas. Então, houve a necessidade de padronizar o algoritmo de cifragem por computadores. Desse modo, o NBS (National Bureau of Standards) americano solicitou propostas para um sistema padrão de ciframento de dados e, em 1976, adotou o DES (Data Encryption Standard) - desenvolvido por pesquisadores da IBM. Tal adoção foi permitida pela NSA, que também era responsável pelo controle do uso da criptografia computacional com fins não ligados à segurança nacional. Descreveremos o funcionamento do DES no próximo capítulo.

A adoção da cifra DES resolveu o problema do estabelecimento de uma cifra padrão para a comunicação entre as empresas. Além disso, ofereceu à elas um alto nível de segurança, protegendo-as contra ataques de empresas rivais. Apesar disso, a cifra DES mantinha o velho problema da distribuição de chaves: duas partes que quisessem se comunicar com segurança, precisavam se encontrar para combinar a chave.

Incomodado com esse problema - inerente aos cripto-sistemas até então desenvolvidos - Whitfield Diffie, criptógrafo americano, esteve se dedicando à procura de uma solução na década de 70. Nessa época, os EUA já possuiam computadores militares interligados, permitindo a troca de mensagens entre locais distantes. Para Diffie esse era o prenúncio do desenvolvimento de uma grande rede de computadores conectados, atendendo os interesses da população. Fato que motivou bastante seu desejo de solucionar o problema.

Diffie, em parceria com Martin Hellman - da Universidade de Stanford - e, independentemente, Ralph Merkle - da Universidade da Califórnia - introduziram em 1976 a idéia de cripto-sistema de chave pública.

Tal idéia consistia em estabelecer um sistema que possuisse uma chave de codificação, que pudesse ser divulgada para todo mundo, ou seja, uma chave pública. Além disso, para a transformação da mensagem, seria necessário também uma função unidirecional com segredo. Isto é, uma função tal que dado x é fácil calcular $f(x)$, mas dado $f(x)$ é intratável calcular x quando não se conhece o segredo. Assim, nesse sistema, o conhecimento da função e da chave que possibilitam o ciframento, não comprometeria o sigilo da mensagem. Apenas o destinatário legítimo conheceria o segredo que permite a inversão da função de ciframento, que seria sua chave secreta de deciframento. A figura 2.5 esquematiza um cripto-sistema de chave pública.

Figura 2.5: Esquema de um cripto-sistema de chave pública.

Apesar de Diffie, Hellman e Merkle terem concebido a idéia geral de cripto-sistema de chave pública, não tinham uma função que preenchesse os critérios. A partir daí, os cientistas concentraram na busca de uma função apropriada.

A princípio um forte candidato foi um sistema criptográfico, desenvolvido por Merkle e Hellman, baseado no problema da mochila. Tal problema consiste em estabelecer quais elementos de um determinado conjunto devem ser somados para dar como resultado um

valor S. Porém o cripto-sistema MH - como ficou conhecido - mostrou-se frágil e foi quebrado no início da década de 80 por Adi Shamir, cientista da computação. Descreveremos esse cripto-sistema no capítulo 4.

O problema foi resolvido, por um trio de cientistas na Costa Leste dos Estados Unidos, após um ano de pesquisa. Rivest, Shamir e Adleman, baseando-se em uma transformação exponencial, desenvolveram o RSA, um dos métodos mais usados em aplicações comerciais até hoje.

Veremos no capítulo 4 que a segurança do RSA está na dificuldade de fatoração de um produto de dois primos grandes. Observe que é fácil calcular o produto de dois primos da ordem de 10^{150}, por exemplo, porém a fatoração de tal produto levaria hoje, utilizando um supercomputador, milhares de anos. Isso porque não se conhece um algoritmo rápido para realizar essa tarefa.

Os indianos Manindra Agrawal, Neeraj Kayal e Nitin Saxena desenvolveram em 2002, um algoritmo capaz de determinar se um número n é primo ou composto em tempo polinomial. Em outras palavras, o número de passos computacionais necessários para tal determinação pode ser estimado calculando-se o valor de um polinômio, $p(m)$, onde m é o número de algarismos de n. Por esse motivo, o algoritmo é considerado bem mais rápido do que os até então utilizados para determinar a primalidade de um número. Essa descoberta não afeta imediatamente a segurança do RSA que, como dissemos, depende do conhecimento dos fatores primos de um número. Porém causa preocupação por parte dos usuários desse sistema criptográfico.

Além disso, a segurança do RSA pode ser comprometida caso pesquisadores consigam desenvolver computadores baseados nos princípios da mecânica quântica. Dessa forma, a velocidade de processamento da informação aumentaria significativamente, o que tornaria os cálculos muito mais rápidos, diminuindo o tempo necessário na fatoração.

Por enquanto, com a descoberta do RSA, os criptógrafos estão vencendo a "guerra da informação" estabelecida no decorrer da evolução da criptografia.

2.2 A importância do uso da criptografia

Ao longo da história, o uso da criptografia permitiu a troca de mensagens secretas entre amantes, espiões, chefes de estado, enfim entre todas as pessoas que desejavam se comunicar com privacidade. Além disso, possibilitou que informações importantes - como dados dos Estados, descobertas científicas, localização de tesouros, etc. - fossem protegidas, ou seja, mantidas em segredo. Entretanto, seu uso se fez de maneira mais significativa nas áreas militares e diplomáticas dos governos. Nesses setores a informação, na maioria das vezes, é um bem bastante precioso a ser protegido com as melhores "armas" existentes.

No último século, o grande desenvolvimento da tecnologia tornou a comunicação rápida. Atualmente, a internet, por exemplo, facilita o envio e o recebimento de mensagens por meio do correio eletrônico, permite efetuar transações bancárias, bem como realizar compras com cartão de crédito. Caixas eletrônicos (ATMs - Automatic Teller Machines) oferecem serviços como pagamentos, saques e transferências, através do uso de um cartão plástico e uma senha. A urna eletrônica promove um processo de eleição eficaz e agiliza a transmissão dos votos.

Por outro lado, o avanço da eletrônica aumentou a vulnerabilidade das informações,

uma vez que as mensagens passaram a ser transmitidas através de sinais digitais que trafegam ao longo de redes públicas de comunicação. Tais sinais podem ser captados e modificados facilmente comprometendo a segurança dos usuários de um determinado sistema.

Assim, a criptografia se faz cada vez mais necessária para garantir o sigilo, a integridade e a autenticação das mensagens.

Capítulo 3

Cripto-sistemas de chave secreta

Consideraremos neste capítulo alguns cripto-sistemas de chave secreta. Nesses cripto-sistemas os usuários devem manter a chave de ciframento em segredo, uma vez que a chave de deciframento é igual à ela ou é facilmente obtida a partir da mesma.

Iniciaremos com alguns exemplos de cifras de transposição e, em seguida, apresentaremos as principais cifras de substituição. Por último, faremos uma descrição da cifra DES (Data Encryption Standard), um cripto-sistema composto com fins nas aplicações computacionais.

3.1 Transposições

As transposições consistem em permutar as letras de uma mensagem reordenando-as de acordo com um determinado esquema, previamente combinado entre o remetente e o destinatário.

A reordenação das letras pode ser feita de várias maneiras, em seguida, comentaremos algumas delas.

3.1.1 Cerca de ferrovia

Esse padrão de ciframento consiste em escrever a mensagem de forma que as letras alternadas fiquem separadas em duas linhas. Após a separação das letras, escrevemos a seqüência de letras da linha superior seguida da seqüência de letras da linha inferior.

Exemplo:

Mensagem original: `esconda a localização do tesouro`

Transformação:

```
e c n a l c l z ç o o e o r
 s o d a o a i a a d t s u o
```

Mensagem cifrada: `ECNALCLZÇOOEORSODAOAIAADTSUO`

Ao receber a mensagem cifrada o destinatário poderá recuperar a mensagem original revertendo o processo.

Note que poderíamos utilizar esse padrão com 3 ou mais linhas. Desse modo, o número de linhas utilizados constituiria a chave de ciframento e deciframento do sistema.

3.1.2 Cifra de transposição colunar

Nesta cifra a mensagem original é escrita em uma matriz, linha por linha. Em seguida as colunas da matriz são permutadas e a mensagem cifrada é removida, coluna por coluna.

As dimensões da matriz e a permutação das colunas determinam a chave da cifra.

Exemplo:

Mensagem original: `corram para o leste`

Chave: matriz 4×4 e a permutação $3 - 1 - 2 - 4$ para as colunas.

Transformação:

1	2	3	4		3	1	2	4
c	o	r	r		R	C	O	R
a	m	p	a	$\longrightarrow$	P	A	M	A
r	a	o	l		O	R	A	L
e	s	t	e		T	E	S	E

Mensagem cifrada: `RPOTCAREOMASRALE`

O receptor, ciente da chave usada na codificação, poderá recuperar a mensagem original revertendo o processo.

Uma outra forma de transposição semelhante à essa é a cifra de permutação periódica que descreveremos em seguida.

3.1.3 Cifra de permutação periódica

De maneira geral, para criptografarmos pela cifra de permutação periódica, dividimos a mensagem em blocos de tamanho d. Além disso, consideramos uma permutação $f : \mathbb{Z}_d \to \mathbb{Z}_d$ onde $\mathbb{Z}_d$ representa os inteiros de 1 a d. Assim, cada bloco de d letras será permutado de acordo com f.

Isso significa que uma mensagem original

$$m_1 m_2 \cdots m_d \quad m_{d+1} \cdots m_{2d} \quad \cdots$$

é cifrada como

$$m_{f(1)} m_{f(2)} \cdots m_{f(d)} \quad m_{d+f(1)} \cdots m_{d+f(d)} \quad \cdots .$$

Exemplo:

Mensagem original: `corram para o leste`

Chave: $d = 4$ e a permutação

$$i : 1 \;\; 2 \;\; 3 \;\; 4$$

$$f(i) : 4 \;\; 2 \;\; 1 \;\; 3$$

Transformação:

`corr ampa raol este`

`ROCR AMAP LARO ESET`

Mensagem cifrada: `ROCRAMAPLAROESET`

Para decifrar o destinatário usará a permutação inversa.

De forma análoga à cifra de transposição colunar, podemos ver a cifra de permutação periódica como transposições das colunas de uma matriz em que a mensagem foi escrita linha por linha. A diferença é que, no caso da cifra de permutação periódica, a mensagem cifrada é extraída linha por linha e não coluna por coluna como fizemos na subseção anterior.

A cifra de permutação periódica é considerada mais eficiente para aplicações computacionais do que a cifra de transposição colunar. Isso porque cada linha pode ser cifrada e decifrada de forma independente.

Um criptoanalista identifica um texto cifrado como resultado de uma transposição, comparando a freqüência relativa das letras na mensagem cifrada à freqüência de ocorrência das letras do alfabeto no idioma. Além disso, a quebra das cifras de transposição não é muito difícil, podendo ser feita baseando-se na freqüência de digramas (pares ordenados de letras) e trigramas (triplas ordenadas de letras) no idioma da mensagem.

3.2 Substituições

Nesta seção apresentaremos descrições, exemplos e generalizações de alguns métodos de substituição das letras de uma mensagem por outras.

Com isso, esperamos entre outros aspectos, evidenciar a principal diferença entre as cifras de substituição monoalfabéticas e polialfabéticas - fato da substituição depender da posição da letra na mensagem ou não -, bem como mostrar algumas relações existentes entre os métodos de criptografia e conceitos da álgebra.

3.2.1 Cifras de substituição monoalfabéticas

Nas cifras de substituição monoalfabéticas cada letra do texto original é substituída sempre pela mesma letra, qualquer que seja sua posição. Essa substituição pode ser feita de acordo com uma tabela - previamente combinada entre o remetente e o destinatário -

que estabelece uma correspondência 1 a 1 entre o alfabeto original e uma versão misturada do mesmo, denominada alfabeto cifrado.

Observe que para um alfabeto de 26 letras, são 26! possibilidades diferentes de tabelas, que podem ser construídas de maneira aleatória, ou a partir de alguma regra, como a tabela 2.1 do capítulo 2. Em seguida, discutiremos o conjunto de substituições monoalfabéticas baseado nas transformações afins em $\mathbb{Z}_{26}$.

Cifra de César

Conforme descrevemos no capítulo 2, a cifra de César consiste em substituir cada letra de uma mensagem por outra, localizada três posições à frente no alfabeto.

Exemplo:

Mensagem original: `ataquem ao amanhecer`

Transformação:

`ataquemaoamanhecer`

`DWDTXHPDRDPDQKHFHU`

Mensagem cifrada: `DWDTXHP DR DPDQKHFHU`

A partir da correspondência entre letras e números estabelecida na tabela 2.2, podemos descrever a cifra de César matematicamente através da relação

$$c = m + 3, \ em \ \mathbb{Z}_{26},$$

onde m é o número de uma letra da mensagem original e c é o número da letra correspondente na mensagem cifrada.

Para decifrar basta aplicarmos a relação inversa

$$m = c - 3, \ em \ \mathbb{Z}_{26}.$$

A cifra de César é um caso particular de um conjunto de cifras de deslocamento dado pela relação

$$c = m + k, \ em \ \mathbb{Z}_{26},$$

onde $0 \square k \square 25$.

Note que essa relação considera 26 possibilidades de deslocamento para as letras de uma mensagem, incluindo o caso $k = 0$, onde as letras não são alteradas. Tais possibilidades representam as chaves da cifra.

Transformações afins

Podemos generalizar ainda mais considerando as cifras baseadas nas transformações afins, nas quais a substituição das letras é determinada pela relação

$$c = am + b, \ em \ \mathbb{Z}_{26},$$

onde a e b são inteiros com $0 \square a,\ b \square 25$ e $mdc(a, 26) = 1$.

Observe que caso usássemos valores de a tais que $mdc(a, 26) \neq 1$ teríamos letras diferentes sendo cifradas por letras iguais, o que representaria um grande problema na decifragem. Além disso, algumas letras não apareceriam no alfabeto cifrado.

Por exemplo, na relação $c = 10m + 1$, as letras `a` e `n` são cifradas como `B` e, em conseqüência, `B` será decifrado como `A` e `N`. Por outro lado, utilizando essa relação, a letra `O` não aparece no texto cifrado.

Portanto, a condição $mdc(a, 26) = 1$ deve ser satisfeita para que possamos estabelecer uma correspondência 1 a 1 entre o alfabeto padrão e o alfabeto cifrado. Com isso, será possível decifrar corretamente cada letra da mensagem cifrada.

De fato, se $mdc(a, 26) = 1$ então, pela proposição 1.1.1 do capítulo 1, $\exists a^{-1}$ em $\mathbb{Z}_{26}$. Donde é fácil ver que a transformação $c = am + b$ é injetiva em $\mathbb{Z}_{26}$.

Assim, podemos decifrar cada letra da mensagem de maneira única fazendo

$$m = a^{-1}(c - b),\ em\ \mathbb{Z}_{26}.$$

O par de valores a e b representa a chave da cifra. Observe que há 12 possibilidades para a, pois $\mathbb{Z}_{26}$ possui $\Phi(26) = 12$ elementos invertíveis, e 26 possibilidades para b. Isso nos dá $12 \cdot 26 = 312$ transformações possíveis. Entre essas, podemos destacar a cifra de César, quando $a = 1$ e $b = 3$, e o caso $a = 1$ e $b = 0$, que representa a transformação $c = m$ em $\mathbb{Z}_{26}$, que não altera a mensagem original.

Exemplo:

Mensagem original: `quero te encontrar hoje à noite`

Chave: $a = 3$ e $b = 5$.

Essa chave nos fornece a seguinte correspondência entre as letras do alfabeto original e do alfabeto cifrado:

Tabela 3.1: Correspondência entre as letras para uma transformação afim $c = 3m + 5$.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
5	8	11	14	17	20	23	0	3	6	9	12	15
F	I	L	O	R	U	X	A	D	G	J	M	P
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25
18	21	24	1	4	7	10	13	16	19	22	25	2
S	V	Y	B	E	H	K	N	Q	T	W	Z	C

Mensagem cifrada: `BNREV KR RSLVSKEFE AVGR F SVDKR`

Para decifrar essa mensagem, o receptor utilizará a relação

$$m = a^{-1}(c - b)$$

com $a^{-1} = 9$ e $b = 5$.

Assim, para encontrar a primeira letra da mensagem original, ele deverá calcular:

$$m = 9(1-5) \Rightarrow m = 9(-4) \Rightarrow m = -36 \Rightarrow m = 16,$$

que corresponde à letra `q`. Analogamente, as demais letras da mensagem original são encontradas.

Cifras baseadas nas substituições afins são facilmente quebradas pois, como vimos, são apenas 312 possibilidades de escolha para a e b. Dessa forma, se um criptoanalista decidisse testar as chaves possíveis, não levaria muito tempo para encontrar a chave correta e decifrar a mensagem.

Uma outra alternativa de criptoanálise tem como base a análise da freqüência das letras no texto cifrado.

Para exemplificar esse método, consideremos a mensagem em português, cifrada através de uma relação afim:

`EERVMNOBEFMYZOLNEAZKTKZQMXGKAMXGMOXTEZQKYE`

`MGMOQLMFOZSUMELEXMXNMGFMGYURZKQGMUYEXNMUFE`.

Nosso primeiro passo deve ser contar o número de vezes que cada letra aparece na mensagem, estabelecendo uma tabela de ocorrência:

Tabela 3.2: Número de ocorrência das letras na mensagm cifrada.

A	2	F	4	K	5	P	0	U	4	Z	6
B	1	G	6	L	3	Q	4	V	1		
C	0	H	0	M	14	R	2	W	0		
D	0	I	0	N	4	S	1	X	6		
E	10	J	0	O	5	T	2	Y	4		

Observando a freqüência das letras no texto cifrado, podemos estabelecer algumas hipóteses.

Como as letras mais comums no idioma da mensagem são `a, e` e `o`, nessa ordem, podemos supor que as letras `M` e `E` do texto cifrado representam, respectivamente, as letras `a` e `e` da mensagem original.

Dessa forma, como a transformação é feita através de uma relação da forma $c = am+b$, em $\mathbb{Z}_{26}$, podemos estabelecer o seguinte sistema de equações em $\mathbb{Z}_{26}$:

$$\begin{cases} 0a + b = 12 \\ 4a + b = 4 \end{cases}$$

donde, $b = 12$ e $4a = 18$.

Essa última equação possui como solução $a = 11$ e $a = 24$, mas como $a \in U(26)$ consideraremos apenas $a = 11$. Assim, como $a^{-1} = 19$ tentaremos decifrar o texto com a relação:

$$m = 19(c - 12), \ em\mathbb{Z}_{26}.$$

Porém, ao empregarmos essa relação para decifrar as primeiras letras da mensagem, observamos que não estamos indo pelo caminho correto. Isso porque obtemos a sequência de letras "`eerpatmzexauno...`" que não faz sentido algum.

Podemos fazer outras suposições como, por exemplo, que `M` e `E` do texto cifrado correspondem, respectivamente, às letras `e` e `a` ou `a` e `o`, mas em nenhum dos dois casos obtemos resultados satisfatórios.

Façamos uma outra tentativa. Dessa vez, vamos supor que a letra `M` corresponde à letra `e` e a letra `E` corresponde à letra `o`. Assim, obtemos o seguinte sistema de equações em $\mathbb{Z}_{26}$:

$$\begin{cases} 4a + b = 12 \\ 14a + b = 4 \end{cases}$$

Multiplicando a primeira equação por -1 e somando as duas equações obtemos a relação $10a = 18$, cujas soluções, em $\mathbb{Z}_{26}$, são $a = 7$ e $a = 20$. Novamente, como $a \in U(26)$, consideraremos apenas a solução $a = 7$. Dessa forma, $b = 10$ e a tentativa de decodificação deverá ser feita através da relação:

$$m = 15(c - 10),$$

pois $a^{-1} = 15$, em $\mathbb{Z}_{26}$.

Aplicando a relação acima aos números correspondentes das letras da mensagem cifrada, obtemos:

`ooobjetivodecriptografarmensagenseinformaco`

`eseimpedirqueoponentesdescubramseuconteudo`

Inserindo os espaçamentos necessários, finalizamos o processo de criptoanálise obtendo a mensagem original:

"`o objetivo de criptografar mensagens e informações é impedir que oponentes descubram seu conteúdo`".

3.2.2 Cifras de substituição polialfabéticas

Como vimos no capítulo 2, nas cifras de substituição polialfabéticas letras iguais da mensagem original podem ser substituídas por letras diferentes, dependendo da sua posição no texto. Com isso, a freqüência de letras individuais não é preservada, fato que representa uma grande vantagem em relação às cifras de substituição monoalfabéticas.

Em seguida, estudaremos a cifra de Vigenère, um dos mais antigos e conhecidos criptosistemas de substituição polialfabética. Estudaremos também a cifra de Hill, um sistema criptográfico que realiza a substituição através de uma transformação matricial.

Cifra de Vigenère

A cifra de Vigenère consiste em estabelecer uma seqüência de letras $l_1 l_2 \cdots l_n$, com números equivalentes a $k_1, k_2, \cdots, k_n$, que servirá como chave.

Em seguida, dividimos a mensagem original em blocos de n letras com números equivalentes a $m_1, m_2, \cdots, m_n$, de acordo com a tabela 2.2.

Para obtermos as letras da mensagem cifrada, de números equivalentes a $c_1, c_2, \cdots c_n$, usaremos a seguinte relação em $\mathbb{Z}_{26}$:

$$c_i = m_i + k_i,$$

para $i = 1, 2, \cdots, n$.

Dessa forma, cada letra da mensagem original, de número equivalente a m_i é deslocada de k_i posições. Em outras palavras, para cada letra empregamos um deslocamento diferente.

Note que em particular, quando $n = 1$, a cifra é uma substituição monoalfabética, ou melhor, uma generalização da cifra de César para um determinado deslocamento. Por outro lado, quando n é do tamanho do texto, obtemos a cifra one-time pad mencionada no capítulo 2.

Antes de exemplificarmos a cifra de Vigenère, vamos apresentar o quadrado de Vigenère, um esquema que facilita o processo de ciframento e deciframento de mensagens.

Tabela 3.3: Quadrado de Vigenère.

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

Nesse quadrado, cada linha representa um alfabeto cifrado de acordo com um deslocamento de 0 a 25 posições para as letras do alfabeto original.

Exemplo:

Mensagem original: `desloque as tropas para o sul`

Chave: secreto

Transformação:

desloqu	eastrop	asparao	sul
secreto	secreto	secreto	sec
VIUCSJI	WEUKVHD	SWRRVTC	KYN

Mensagem cifrada: `VIUCSJIWEUKVHDSWRRVTCKYN`

Observe que a primeira letra de cada grupo de sete letras da mensagem original foi deslocada 18 posições, a segunda letra 4 posições, e assim por diante, de acordo com a correspondência entre letras e números dada na tabela 2.2.

Pelo quadrado de Vigenère, para cifrar a letra `d` da mensagem, com a letra `s` da chave, devemos localizar a letra da coluna "d" com a linha "S", para cifrar a letra `e` da mensagem, com a letra `e` da chave, localizamos a letra da coluna "e" com a linha "E", e assim por diante. Em suma, pelo quadrado de Vigenère, cada letra da mensagem cifrada é localizada na coluna da letra da mensagem original com a linha da letra correspondente da chave.

Para decifrar a mensagem através do quadrado de Vigenère, o receptor deverá localizar na linha da letra correspondente da chave a letra da cifra, assim, será possível encontrar no topo da coluna a letra da mensagem original.

Vejamos como criptoanalisar uma mensagem codificada pela cifra de Vigenère. Nos basearemos no método desenvolvido por Babbage referido no capítulo 2.

Consideremos a mensagem:

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

O primeiro passo da criptoanálise, consiste em procurar por seqüências de letras repetidas no texto cifrado. Essas seqüências podem surgir principalmente do uso de uma mesma parte da chave para cifrar a mesma seqüência de letras no texto original. Pode ainda acontecer, mais raramente, de seqüências diferentes no texto original serem cifradas

com partes diferentes da chave, originando seqüências iguais na mensagem cifrada. Essa última situação será desconsiderada.

Vemos na mensagem acima que a seqüência `EGJADC` aparece três vezes no texto cifrado e que a seqüência `HCT` aparece duas vezes.

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

Observando os espaçamentos entre as repetições dessas duas seqüências temos que:

1) A seqüência `EGJADC` aparece pela segunda vez após 20 letras da primeira aparição.

2) A seqüência `EGJADC` aparece pela terceira vez após 56 letras da segunda aparição.

3) A seqüência `HCT` repete após 44 letras.

Dessa forma, podemos estabelecer algumas hipóteses em relação ao tamanho da chave, considerando os divisores dos números de letras entre as repetições.

Assim, de **1)** podemos supor que o tamanho da chave é $1, 2, 4, 5, 10$ ou 20. De **2)** o tamanho da chave pode ser $1, 2, 4, 7, 8, 14, 28$ ou 56. E, por último, de **3)** a chave é de $1, 4$ ou 11 letras.

Com isso, percebemos que todos os espaçamentos são divisíveis por 4. Donde consideraremos, essa possibilidade com mais cuidado.

Supondo que a chave possui 4 letras e que a 1ª letra da mensagem foi cifrada com a 1ª letra da chave, a 2ª letra da mensagem foi cifrada com a 2ª letra da chave, e assim por diante, temos que as letras que ocupam as posições $1, 5, 7, \cdots$, assim como as letras que ocupam as posições $2, 6, 10, \cdots$, etc., foram cifradas utilizando a mesma linha do quadrado de Vigenère.

Como cada linha corresponde a um deslocamento entre 0 e 25, poderemos considerar cada um dos quatro grupos de letras como uma substituição monoalfabética simples e, assim, realizar a análise de freqüências.

Procedendo dessa forma, o criptoanalista rapidamente chegará à mensagem:

```
a c r i p t o g r a f i a e u m a l u t
a e n t r e a p e s s o a q u e c o d i
f i c a e a s p e s s o a s d e s a u t
o r i z a d a s q u e t e n t a m q u e
b r a r a c i f r a d e s s e m o d o p
e s s o a s d e s a u t o r i z a d a s
s a o i n i m i g o s a s e r e m c o m
```

```
b a t i d o s c o m a s m e l h o r e s
a r m a s d i s p o n i v e i s
```

Cuja chave utilizada foi a palavra `CRIP`.
Inserindo espaçamentos e acentuação adequados obtemos:

"a criptografia é uma luta entre a pessoa que codifica e as pessoas desautorizadas que tentam quebrar a cifra desse modo pessoas desautorizadas são inimigos a serem combatidos com as melhores armas disponíveis".

Note que a criptoanálise da cifra de Vigenère é fundamentada no uso periódico da chave. A partir do conhecimento do tamanho da chave é possível separar a mensagem em blocos e analisar a freqüência das letras considerando posição por posição nos mesmos. Dessa forma, a criptoanálise se torna tão simples quanto a de uma substituição monoalfabética.

Particularmente, se a chave possuir um número de letras igual ao do texto, e for gerada ao acaso, a cifra (one-time pad) é inquebrável. Assim, a cifra de Vigenère é eficiente somente quando o fluxo de informações é pequeno, pois só é possível garantir a sua segurança considerando chaves de comprimento igual ao do texto.

Cifra de Hill

Na cifra de Hill, a mensagem original também é dividida em blocos de n letras, de números equivalentes a $(m_1, m_2, \cdots, m_n)$, dados pela tabela 2.2, como no ciframento de Vigenère. Porém, as letras da mensagem cifrada $(c_1, c_2, \cdots, c_n)$, em $\mathbb{Z}_{26}$, são tais que c_i é uma combinação linear de $(m_1, \cdots, m_n)$, $\forall i$ tal que $1 \square i \square n$. Isto é,

$$c_1 = a_{11}m_1 + \cdots + a_{1n}m_n$$

$$c_2 = a_{21}m_1 + \cdots + a_{2n}m_n$$

$$\vdots$$

$$c_n = a_{n1}m_1 + \cdots + a_{nn}m_n,$$

com $a_{ij} \in \mathbb{Z}_{26}$.

Utilizando a notação de matrizes temos:

$$C = AM,$$

onde

$$C = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix},\ A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}\ e\ M = \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix}$$

são matrizes com entradas em $\mathbb{Z}_{26}$.

Para que seja possível decifrar uma mensagem codificada pela cifra de Hill, é necessário que a matriz A seja invertível. Isso significa, em conseqüência do teorema 1.1.1 e da proposição 1.1.1, que $mdc(detA, 26) = 1$. Assim, se o determinante da matriz A satisfaz essa condição, podemos multiplicar ambos os lados da equação $C = AM$ por A^{-1}, obtendo

$$M = A^{-1}C,$$

que fornecerá a mensagem original de volta.

Exemplo:

Para ilustrarmos essa cifra, consideraremos $n = 2$, isso significa que a mensagem original será dividida em blocos de 2 letras.

Mensagem original: `o ouro está enterrado no norte`

Chave: matriz $A = \begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix} \in M_2(\mathbb{Z}_{26})$.

Transformação:
Dividindo a mensagem em blocos de duas letras temos:

`oo ur oe st ae nt er ra do no no rt ex,`

note que para completar o último par foi necessário acrescentar a letra `x`.

Colocando o número correspondente a cada letra de acordo com a tabela 2.2, temos:

14 14 20 17 14 4 18 19 0 4 13 19 4 17 17 0 3 14 13 14 13 14 17 19 4 23

Em seguida, fazemos a multiplicação dos números correspondentes a cada par de letras, escritos na forma de matriz coluna, pela matriz $A = \begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix}$.

Dessa forma, o primeiro par de letras é cifrado como:

$$C = \begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix} \begin{bmatrix} 14 \\ 14 \end{bmatrix} = \begin{bmatrix} 5 \cdot 14 + 17 \cdot 14 \\ 4 \cdot 14 + 15 \cdot 14 \end{bmatrix} = \begin{bmatrix} 22 \\ 6 \end{bmatrix},$$

que corresponde ao par de letras `WG`.

O segundo par de letras é cifrado como:

$$C = \begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix} \begin{bmatrix} 20 \\ 17 \end{bmatrix} = \begin{bmatrix} 5 \cdot 20 + 17 \cdot 17 \\ 4 \cdot 20 + 15 \cdot 17 \end{bmatrix} = \begin{bmatrix} 25 \\ 23 \end{bmatrix}$$

que corresponde ao par de letras `ZX`.

Analogamente, criptografamos os demais pares obtendo os números:

22 6 25 23 8 12 23 19 16 8 24 25 23 11 7 16 19 14 17 2 17 2 18 15 21 23

que correspondem aos seguintes pares de letras:

WG ZX IM XT QI YZ XL HQ TO RC RC SP VX

Mensagem cifrada: WGZXIMXTQIYZXLHQTORCRCSPVX.

Na decifragem, o receptor deverá utilizar a matriz

$$A^{-1} = \begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix},$$

inversa da matriz A, calculando $M = A^{-1}C$, para cada par de letras da mensagem cifrada.

Dessa forma, o primeiro par, por exemplo, será decifrado como:

$$M = \begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix} \begin{bmatrix} 22 \\ 6 \end{bmatrix} = \begin{bmatrix} 14 \\ 14 \end{bmatrix},$$

que corresponde ao par de letras oo, como esperávamos.

A criptoanálise da cifra de Hill é baseada no conhecimento das letras originais de partes do texto cifrado. Para ilustrar como ela é feita, consideraremos um ciframento também realizado dividindo-se a mensagem em blocos de duas letras.

Suponha que o criptoanalista saiba que a mensagem foi cifrada em blocos de 2 letras e que os pares de letras (m_1, m_2) e (m'_1, m'_2), correspondam, respectivamente, aos pares (c_1, c_2) e (c'_1, c'_2) do texto cifrado. Observe que isso pode ser descoberto associando-se os digramas mais freqüentes do texto cifrado aos digramas mais comuns no idioma da mensagem.

Escrevendo esses blocos como matrizes coluna e considerando a relação

$$M = A^{-1}C,$$

temos

$$\begin{bmatrix} m_1 \\ m_2 \end{bmatrix} = A^{-1} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} \; e \; \begin{bmatrix} m'_1 \\ m'_2 \end{bmatrix} = A^{-1} \begin{bmatrix} c'_1 \\ c'_2 \end{bmatrix}$$

ou seja,

$$\begin{bmatrix} m_1 & m'_1 \\ m_2 & m'_2 \end{bmatrix} = A^{-1} \begin{bmatrix} c_1 & c'_1 \\ c_2 & c'_2 \end{bmatrix}.$$

Se a matriz

$$\begin{bmatrix} c_1 & c'_1 \\ c_2 & c'_2 \end{bmatrix}$$

for invertível em $M_2(\mathbb{Z}_{26})$, isto é, se $mdc(det(C), 26) = 1$, o criptoanalista poderá multiplicar ambos os lados da última igualdade por

$$C^{-1} = \begin{bmatrix} c_1 & c'_1 \\ c_2 & c'_2 \end{bmatrix}^{-1},$$

obtendo a matriz A^{-1}, que possibilitará a decifração completa da mensagem.

Por outro lado, se a matriz C não for invertível, a criptoanálise não será tão rápida.

Suponha, por exemplo, que os digramas NS e HI sejam, nessa ordem, os mais freqüentes

num texto, criptografado pela cifra de Hill, que desejamos criptoanalisar. Caso a mesagem original seja em português, como os digramas `DE` e `RA` são os mais comuns nesse idioma, podemos supor que `NS` corresponde a `DE` e `HI` corresponde a `RA`.

Dessa forma, os pares $(3,4)$ e $(17,0)$ foram transformados em $(13,18)$ e $(7,8)$, respectivamente.

Assim, temos:

$$\begin{bmatrix} 3 & 17 \\ 4 & 0 \end{bmatrix} = A^{-1} \begin{bmatrix} 13 & 7 \\ 18 & 8 \end{bmatrix}.$$

Como a matriz

$$C = \begin{bmatrix} 13 & 7 \\ 18 & 8 \end{bmatrix}$$

não é invertível em $M_2(\mathbb{Z}_{26})$, pois $det(C) = 4$ e $mdc(4,26) = 2$, podemos tentar obter uma matriz invertível através de outro par de letras. Caso não seja possível, uma outra alternativa consiste em reduzir o número de possibilidades para essa matriz.

Isso será feito considerando as matrizes:

$$\overline{A}^{-1},\ \overline{M} = \begin{bmatrix} 3 & 4 \\ 4 & 0 \end{bmatrix}\ e\ \overline{C} = \begin{bmatrix} 0 & 7 \\ 5 & 8 \end{bmatrix}$$

que são, respectivamente, as reduções das matrizes A^{-1}, M e $C \in M_2(\mathbb{Z}_{26})$ em $M_2(\mathbb{Z}_{13})$.

Dessa forma, a partir da relação

$$\overline{M} = \overline{A}^{-1}\overline{C}$$

e da inversa de $\overline{C}$ em $M_2(\mathbb{Z}_{13})$ podemos obter

$$\overline{A}^{-1} = \overline{M}\ \overline{C}^{-1} = \begin{bmatrix} 3 & 4 \\ 4 & 0 \end{bmatrix} \begin{bmatrix} 2 & 8 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 11 \\ 8 & 6 \end{bmatrix}.$$

Assim, como as entradas da matriz $\overline{A}^{-1}$, pertencentes a $\mathbb{Z}_{13}$, são reduções das entradas da matriz A^{-1}, pertencentes a $\mathbb{Z}_{26}$, temos duas possibilidades para cada entrada de A^{-1}. Assim, temos $2^4 = 16$ possibilidades para a matriz A^{-1}. Mais precisamente,

$$A^{-1} = \begin{bmatrix} 1 & 11 \\ 8 & 6 \end{bmatrix} + 13A_1$$

onde $A_1 \in M_2(\mathbb{Z}_2)$.

Como A^{-1} é invertível, temos que $mdc(det(A^{-1}), 26) = 1$, donde podemos eliminar 10 das 16 possibilidades para A^{-1}.

Além disso, como

$$A^{-1} \begin{bmatrix} 13 & 7 \\ 18 & 8 \end{bmatrix} = \begin{bmatrix} 3 & 17 \\ 4 & 0 \end{bmatrix}$$

ficam apenas duas possibilidades:

$$A^{-1} = \begin{bmatrix} 1 & 11 \\ 8 & 19 \end{bmatrix}\ ou\ A^{-1} = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}.$$

Finalmente, poderemos determinar a matriz correta realizando a decifragem da mensagem codificada com ambas, e verificando qual delas fornece o resultado satisfatório.

No geral, para criptoanalisar mensagens criptografadas pela cifra de Hill, operando com blocos de n letras, podemos nos basear na freqüência de ocorrência de poligramas (blocos de n letras) no idioma da mensagem original. Porém esse método é viável, apenas para pequenos valores de n. Note que para $n = 10$, por exemplo, existem 26^{10} poligramas, o que torna a análise de freqüência dos mesmos praticamente impossível.

3.3 Ciframento composto: DES

Como afirmamos no capítulo anterior, o DES (Data Encryption Standard) é um padrão de ciframento de dados computacionais composto por transposições e substituições.

Esse padrão cifra blocos de 64 bits (dígitos binários) com uma chave de 64 bits.

A figura 3.1 representa o algoritmo usado para cifrar um bloco.

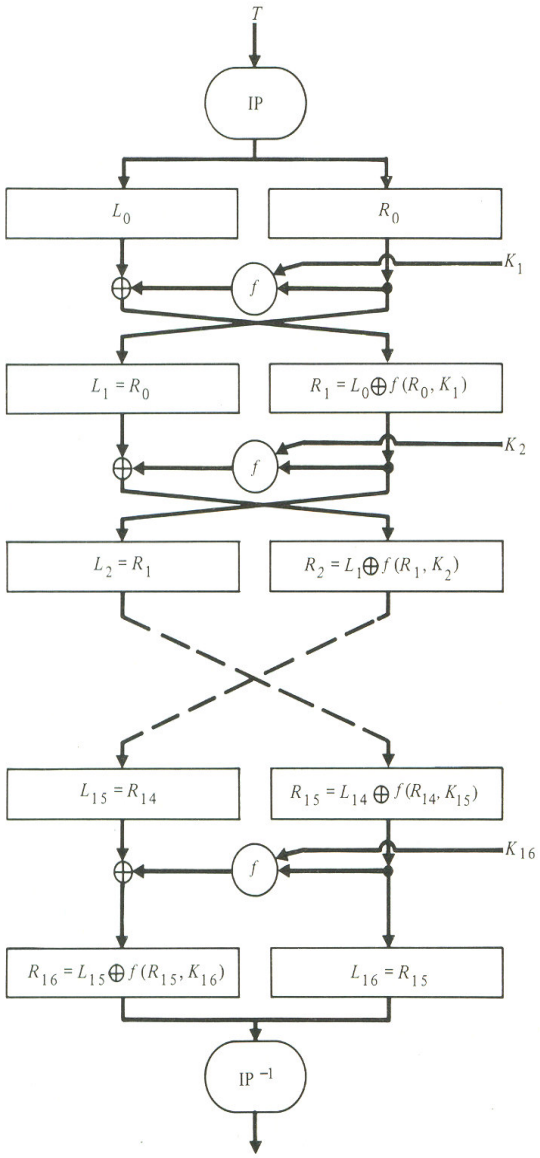

Figura 3.1: Algoritmo de cifragem do DES.

Consideremos um bloco T de 64 bits, numerados de 1 a 64 da esquerda para a direita. O processo de cifragem começa com uma permutação inicial IP desse bloco, dada pela tabela 3.4.

Tabela 3.4: Permutação inicial IP.

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Como resultado obtemos um bloco $T_0 = IP(T)$, também de 64 bits, no qual o primeiro bit é o bit 58 do bloco T, o segundo bit é o bit 50 do bloco T, ..., o último bit é o bit 7 do bloco T. Em outras palavras um bloco $T = t_1 t_2 \cdots t_{64}$ é transposto em $T_0 = t_{58} t_{50} \cdots t_7$.

Em seguida, o bloco T_0 passa por 16 iterações de uma função f que combina substituição e transposição. E, por último, há uma permutação final IP^{-1}, inversa da permutação inicial IP, dada pela tabela 3.5.

Tabela 3.5: Permutação final IP^{-1}.

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Como resultado o algoritmo de cifragem do DES fornece um bloco cifrado, também de 64 bits.

Como dissemos anteriormente, entre a permutação inicial e a final, o algoritmo realiza 16 iterações de uma função f constituída de transposição e substituição.

Em cada iteração i, o bloco T_i resultante é tal que suas metades esquerda e direita, $L_i = t_1 ... t_{32}$ e $R_i = t_{33} ... t_{64}$, respectivamente, são dadas por:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i).$$

Isto é, L_i é exatamente a metade direita, R_{i-1}, do bloco T_{i-1}, resultante da iteração anterior. E R_i é obtido por uma operação $\oplus$ (ou-exclusivo) que representa uma soma, bit a bit em $\mathbb{Z}_2$, da metade esquerda do bloco T_{i-1} com o resultado de uma função f, que

transforma R_{i-1} utilizando uma chave K_i de 48 bits conforme descreveremos em seguida.

Na última iteração, em especial, o bloco $T_{16} = R_{16}L_{16}$. Isso significa que as metades esquerda e direita não são trocadas como nas demais iterações.

O bloco T_{16} encerra o processo de cifragem passando pela permutação final IP^{-1}.

A figura 3.2 esquematiza a função f utilizada na obtenção de R_i na iteração i.

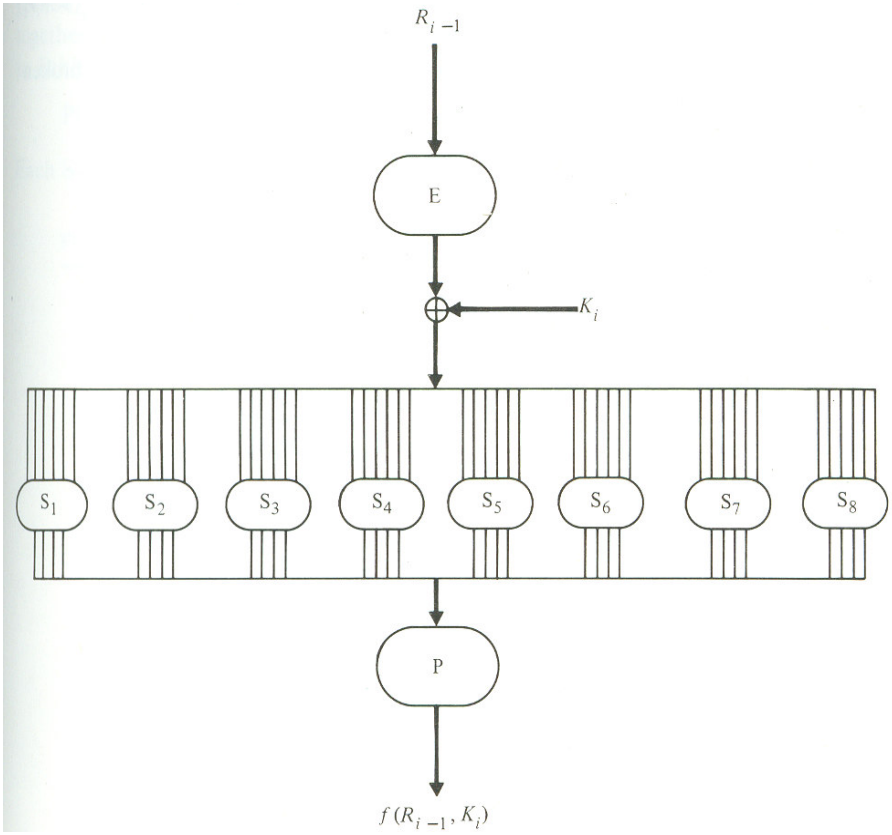

Figura 3.2: Função $f(R_{i-1}, K_i)$.

A função f transforma a metade R_{i-1}, de 32 bits numerados de 1 a 32, expandindo-a para um bloco de 48 bits, $E(R_{i-1})$, de acordo com a tabela 3.6.

Tabela 3.6: Expansão E.

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Note que alguns bits são selecionados mais de uma vez para que ocorra efetivamente

a expansão.

Dessa forma, dado $R_{i-1} = r_1 r_2 \cdots r_{32}$, obtemos $E(R_{i-1}) = r_{32} r_1 r_2 \cdots r_{32} r_1$.

Em seguida, é calculado o ou-exclusivo de $E(R_{i-1})$ com a chave K_i, também de 48 bits. Com isso um novo bloco de 48 bits é obtido. Esse bloco é quebrado em oito blocos de 6 bits, ou seja:

$$E(R_{i-1}) \oplus K_i = B_1 B_2 \cdots B_8$$

onde B_j é um bloco de 6 bits, para 1 □ j □ 8.

Cada um desses 8 blocos passa por um processo de substituição nas caixas S_j, retornando como blocos de 4 bits. Tais substituições são feitas de acordo com a tabela 3.7.

Tabela 3.7: Substituições das caixas S_j.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	S_1
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	S_2
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	S_3
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	S_4
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	S_5
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	S_6
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	S_7
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	S_8
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

Considerando um bloco, $B_j = b_1b_2b_3b_4b_5b_6$, de entrada na caixa S_j, temos que os bits b_1b_6 representam um número entre 0 e 3 que indicará a linha do seu substituto. Por outro lado, os bits $b_2b_3b_4b_5$ representam um número entre O e 15 que indicará a coluna.

Tal substituto é dado por um número inteiro entre 0 e 15. Esse inteiro é escrito na forma binária fornecendo, finalmente, um bloco de 4 bits.

Por exemplo, seja $B_1 = 100011$ o bloco de entrada na caixa S_1. Dessa forma, a saída será o bloco $S_1(B_1) = 1100$, correspondente do inteiro 12, localizado na linha 3 com a coluna 1 de S_1. De fato, $b_1b_6 = 11$, corresponde ao número 3 e $b_2b_3b_4b_5 = 0001$, corresponde ao número 1.

Os oito blocos de 4 bits são reunidos, formando novamente um bloco de 32 bits, que serão transpostos através da permutação P dada pela tabela 3.8.

Tabela 3.8: Permutação P.

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Assim, a determinação de $f(R_{i-1}, K_i)$ é finalizada nos fornecendo como resultado o bloco de 32 bits, $P(S_1(B_1) \cdots S_8(B_8))$.

Como vimos, cada iteração utiliza uma chave K_i de 48 bits. Essas chaves são diferentes, porém derivam de uma mesma chave inicial K de 64 bits, com 8 bits de paridade.

Os bits de paridade são os de posições $8, 16, \cdots, 64$. A permutação $PC-1$, dada na tabela 3.9, os exclui e transpõe os 56 bits restantes.

Tabela 3.9: Permutação $PC-1$ da chave.

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

O resultado da permutação $PC-1$ é então dividido em duas metades C_0 e D_0 de 28 bits. A partir daí, os blocos C_0 e D_0 sofrem um deslocamento circular à esquerda, de uma posição, originando os blocos C_1 e D_1. Por último, a permutação $PC-2$ dada na tabela

3.10 seleciona os 48 bits de K_1, a partir de C_1 e D_1, considerados novamente como um bloco de 56 bits.

Tabela 3.10: Permutação $PC-2$ da chave.

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

De maneira geral, os blocos C_i e D_i, dos quais a permutação $PC-2$ seleciona os bits da chave K_i, são obtidos pelo deslocamento circular à esquerda dos blocos C_{i-1} e D_{i-1}. O número de posições de tal deslocamento é dado na tabela 3.11.

Tabela 3.11: Número de posições dos deslocamentos circulares à esquerda dos blocos C_i e D_i.

Iteração i	deslocamentos circulares de C_i e D_i
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Observe que na 16ª iteração $C_{16} = C_0$ e $D_{16} = D_0$.

A decifragem de dados no DES segue o mesmo algoritmo utilizado na cifragem, invertendo a ordem das chaves. Assim, K_{16} é usada na primeira iteração, K_{15} na segunda, etc. Note que a obtenção do bloco de 64 bits original é possível porque a permutação final IP^{-1} é o inverso da permutação inicial IP. Além disso, temos que:

$$R_{i-1} = L_i$$

$$L_{i-1} = R_i \oplus f(L_i, K_i).$$

Segundo Denning [9], antes da adoção do DES, o NBS (National Bureau of Standards) realizou dois workshops para avaliá-lo. Pesquisadores como Diffie e Hellman estavam preocupados com a fragilidade do sistema.

Apesar da NSA afirmar que o DES era extremamente seguro, após o segundo workshop, alguns cientistas relataram que o DES apresentava duas fraquezas: as caixas S_j e o tamanho da chave.

Em relação às caixas S_j questionou-se a existência de "trapdoors" que funcionariam como "armadilhas" para facilitar a criptoanálise.

Por outro lado, quanto ao tamanho da chave, Diffie e Hellman, conjeturaram a construção de uma máquina que exauriria todas as possibilidades de chaves em apenas um dia.

Acredita-se que a NSA permitiu a adoção do DES com chave de 64 bits para que ela própria fosse capaz de quebrar qualquer mensagem cifrada por ele.

Além disso, na época em que foi adotado, Diffie e Hellman, sugeriram que a segurança do DES estaria garantida para chaves superiores a 112 bits.

Como vimos, cripto-sistemas de chave secreta exigem que o remetente e o destinatário combinem, previamente, a chave a ser utilizada. No entanto, nem sempre é possível fazer isso encontrando-se pessoalmente.

No caso de aplicações computacionais, por exemplo, trafegam pela rede milhões de bits por dia. Isso que significa que diariamente teriam que ser trocados milhões de bits de chave, o que é inviável.

Assim, é necessário confiar em algum outro meio de transmissão de chaves, o que muitas vezes é despendioso e inseguro.

Enfim, a necessidade de uma chave previamente combinada entre o remetente e o destinatário constitui uma das maiores fraquezas dos cripto-sistemas de chave secreta.

No próximo capítulo, estudaremos dois cripto-sistemas do modelo de chave pública que, como afirmamos no capítulo 2, foi desenvolvido com o intuito de contornar o problema da distribuição de chaves, inerente ao modelo de chave secreta.

Capítulo 4

Cripto-sistemas de chave pública

Neste capítulo descreveremos o funcionamento de duas realizações do modelo de chave pública descrito no capítulo 2. Como vimos, ao contrário dos cripto-sistemas de chave secreta, nos cripto-sistemas de chave pública a chave de ciframento pode ser publicada sem comprometer a segurança das informações.

Inicialmente consideraremos o cripto-sistema MH que, embora tenha sido quebrado em 1982 por Shamir, traz uma aplicação algébrica interessante.

Em seguida, apresentaremos o método RSA que faz uso do teorema de Euler, e constitui um dos maiores avanços da criptografia ao longo de toda sua evolução.

4.1 MH

A cifra MH foi proposta na segunda metade da década de 70 por Merkle e Hellman, que se basearam na dificuldade do problema da mochila (*Knapsack problem*).

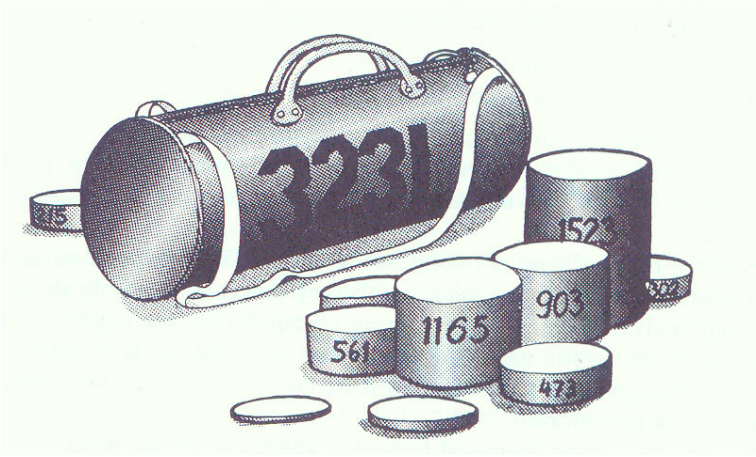

Figura 4.1: Problema da mochila.

Conforme a figura 4.1 sugere, o problema da mochila é: dado um conjunto de inteiros positivos $A = \{a_1, a_2, \cdots, a_n\}$ e o inteiro positivo S, caso seja possível, quais inteiros do conjunto A devem ser adicionados para que o resultado seja S?

Em outras palavras, o problema consiste em estabelecer $x_1, x_2, \cdots, x_n$, com $x_i = 0$ *ou* 1,

para $i = 1, 2, \cdots, n$, tais que

$$S = a_1x_1 + a_2x_2 + \cdots + a_nx_n.$$

Exemplo:

Sejam $A = \{a_1, a_2, \cdots, a_5\} = \{1, 7, 12, 16, 23\}$ e $S = 36$.

Há dois subconjuntos de A cuja soma dos elementos é 36, pois $36 = 1 + 7 + 12 + 16 = 1 + 12 + 23$.

Equivalentemente, podemos dizer que há duas soluções para a equação:

$$36 = 1x_1 + 7x_2 + 12x_3 + 16x_4 + 23x_5,$$

com $x_i = 0$ *ou* 1, para $i = 1, 2, 3, 4, 5$.

São elas: $x_1 = x_2 = x_3 = x_4 = 1, x_5 = 0$, e $x_1 = x_3 = x_5 = 1, x_2 = x_4 = 0$.

Certos valores dos elementos do conjunto A tornam a solução do problema da mochila mais fácil de ser encontrada. Por exemplo, quando consideramos os elementos de A, ordenados como um vetor $(a_1, a_2, \cdots, a_n)$, tais que

$$\sum_{i=1}^{j-1} a_i < a_j,$$

onde $j = 2, 3, \cdots, n$.

Isto é, cada elemento a_j é maior do que a soma dos elementos anteriores. Nesse caso, o vetor $(a_1, a_2, \cdots, a_n)$ é dito **super-crescente**.

Vejamos agora, um exemplo de como o problema da mochila pode ser facilmente resolvido quando trabalhamos com um vetor super-crescente.

Exemplo:

Dado o vetor super-crescente $(2, 5, 9, 17, 32)$ e $S = 43$. Devemos descobrir o vetor $(x_1, x_2, \cdots, x_5)$, com $x_i = 0$ *ou* 1, para $i = 1, 2, 3, 4, 5$, tal que

$$43 = 2x_1 + 5x_2 + 9x_3 + 17x_4 + 32x_5.$$

Inicialmente note que $2 + 5 + 9 + 17 < 32$ e como $S > 32$, então $x_5 = 1$.

Já que $x_5 = 1$, devemos ter $2x_1 + 5x_2 + 9x_3 + 17x_4 = 11$, donde $x_4 = 0$.

Dessa forma, $2x_1 + 5x_2 + 9x_3 = 11 \Rightarrow x_3 = 1$, $x_2 = 0$ e $x_1 = 1$.

Portanto, a solução desse problema é o vetor $(1, 0, 1, 0, 1)$.

No geral, para um vetor $(a_1, a_2, \cdots, a_n)$, super-crescente, e um dado S, podemos resolver o problema da mochila achando os elementos do vetor $(x_1, x_2, \cdots, x_n)$, de acordo com o seguinte algoritmo:

$$x_n = \begin{cases} 1, & \text{se} \quad S \geq a_n \\ 0, & \text{se} \quad S < a_n \end{cases}$$

e,

$$x_j = \begin{cases} 1, & \text{se} \quad S - \sum_{i=j+1}^{n} x_i a_i \geq a_j \\ \\ 0, & \text{se} \quad S - \sum_{i=j+1}^{n} x_i a_i < a_j \end{cases},$$

para $j = n-1, n-2, \cdots, 1$.

Agora que já conhecemos o algoritmo de resolução do problema da mochila, quando esse utiliza um vetor super-crescente, temos ferramenta suficiente para entendermos o cripto-sistema MH.

No cripto-sistema MH, o usuário para quem as mensagens serão destinadas, deve divulgar sua chave pública, constituída de um vetor $(c_1, c_2, \cdots, c_n)$ cujos elementos são inteiros positivos. Merkle e Hellman sugeriram $n = 100$.

O remetente escreve os números binários correspondentes de cada letra da mensagem original. E, em seguida, quebra a mensagem em blocos de n dígitos, $(x_1, x_2, \cdots, x_n)$. Por último, calcula

$$S = \sum_{i=1}^{n} c_i x_i,$$

para cada bloco, e envia os valores encontrados.

Para exemplificarmos, consideraremos a correspondência entre letras e números binários dada na tabela 4.1.

Tabela 4.1: Correspondência entre letras e números binários com cinco dígitos.

a	00000	n	01101
b	00001	o	01110
c	00010	p	01111
d	00011	q	10000
e	00100	r	10001
f	00101	s	10010
g	00110	t	10011
h	00111	u	10100
i	01000	v	10101
j	01001	w	10110
k	01010	x	10111
l	01011	y	11000
m	01100	z	11001

Exemplo:

Mensagem original: `mantenha em sigilo`

Chave pública: $(43, 129, 215, 473, 903, 302, 561, 1165, 697, 1523)$

Transformação:
Inicialmente, escrevemos os números binários correspondentes das letras da mensagem:

`01100 00000 01101 10011`

`00100 01101 00111 00000`

`00100 01100 10010 01000`

`00110 01000 01011 01110`

Em seguida, quebramos a mensagem em blocos de dez dígitos binários e calculamos a soma dos números correspondentes da chave pública, para cada bloco.

Por exemplo, para o primeiro bloco `0110000000`, devemos calcular $129 + 215 = 344$. Para o segundo bloco `0110110011`, calculamos $129+215+903+302+697+1523 = 3769$. E assim por diante.

Isso nos dá os seguintes valores como resultados: 344, 3769, 3464, 1591, 1941, 1077, 1249 e 3928, que serão enviados para o destinatário.

Decifrar a mensagem consiste em determinar a solução do problema da mochila para o vetor $(c_1, c_2, \cdots, c_n)$ e cada uma das somas S enviadas para o destinatário.

Mas, como fazer isso se não exigimos nada do vetor $(c_1, c_2, \cdots, c_n)$? Se $(c_1, c_2, \cdots, c_n)$ fosse super-crescente o problema estaria resolvido, mas isso não é verdade.

Acontece que antes de divulgar $(c_1, c_2, \cdots, c_n)$ o destinatário deve tomar alguns cuidados na escolha desse vetor. Isto é, ele deve escolher um vetor super-crescente $(a_1, a_2, \cdots, a_n)$ e um inteiro positivo $m > 2a_n$. Além disso, deve considerar um inteiro k, tal que $mdc(k, m) = 1$. Assim, estabelece o vetor $(c_1, c_2, \cdots, c_n)$ com $c_j = ka_j$, em $\mathbb{Z}_m$, e $0 \square c_j < m$.

Dessa forma, como $S = \sum_{i=1}^{n} c_i x_i$ e $k \in U(m)$, pois $mdc(k, m) = 1$, temos que

$$k^{-1}S = \sum_{i=1}^{n} k^{-1} c_i x_i = \sum_{i=1}^{n} a_i x_i, em\ \mathbb{Z}_m.$$

Assim, ao receber as somas S, o destinatário calcula $k^{-1}S$ em $\mathbb{Z}_m$, para cada uma delas, transformando o problema inicial da decifragem em um problema equivalente, de fácil resolução pois $(a_1, a_2, \cdots, a_n)$ é super-crescente.

Note que o vetor $(a_1, a_2, \cdots, a_n)$, e os inteiros m e k formam a chave secreta do destinatário.

Exemplo:

Para produzir a chave pública

$$(c_1, c_2, \cdots, c_{10}) = (43, 129, 215, 473, 903, 302, 561, 1165, 697, 1523)$$

do exemplo anterior, foi utilizado o vetor super-crescente

$$(a_1, a_2, \cdots, a_{10}) = (1, 3, 5, 11, 21, 44, 87, 175, 349, 701),$$

$m = 1590$ e $k = 43$.

Dessa forma, para obter a mensagem original de volta, devemos resolver o problema da mochila

$$37 \cdot S = \sum_{i=1}^{10} 37c_i x_i = \sum_{i=1}^{10} a_i x_i, \ em \ \mathbb{Z}_{1590},$$

para $S = 344$, 3769, 3464, 1591, 1941, 1077, 1249 e 3928, pois $k^{-1} = 37$, em $\mathbb{Z}_{1590}$.

Para o primeiro valor de S, por exemplo, temos

$$37 \cdot 344 = 12728 = 8 = 1x_1 + 3x_2 + 5x_3 + 11x_4 + 21x_5 + 44x_6 + 87x_7 + 175x_8 + 349x_9 + 701x_{10}$$

cuja solução é o bloco `0110000000`, correspondendo ao par `MA` de letras.

A princípio, o cripto-sistema MH era um forte candidato a ser amplamente usado como realização do modelo de chave-pública. No entanto, em 1982, Shamir desenvolveu um algoritmo eficiente para resolver o problema da mochila em tempo polinomial.

O algoritmo é baseado no fato de que não é necessário que o criptoanalista ache o correto valor do múltiplo k e de m. É suficiente que ele tenha k' e m', tais que ao multiplicar a seqüência de números que forma a chave pública por k'^{-1} em $\mathbb{Z}_{m'}$ encontre uma seqüência super-cresente. Para mais detalhes veja Salomaa [19].

4.2 RSA

O RSA é um cripto-sistema de chave pública inventado também na segunda metade da década de 70. Seus criadores, Rivest, Shamir e Adleman basearam-se na transformação exponencial

$$C = M^e, \ em \ \mathbb{Z}_n,$$

com $n = pq$, p e q primos grandes e distintos; M inteiro, tal que $1 \square M \square n - 1$; e e um parâmetro, que juntamente com n forma a chave pública, tal que $mdc(e, \Phi(n)) = 1$, onde $\Phi(n) = (p-1)(q-1)$ é a função de Euler.

Para decifrar uma mensagem, é utilizada a chave secreta formada pelos números n e $d = e^{-1}$, em $\mathbb{Z}_{\Phi(n)}$, na relação

$$M = C^d, \ em \ \mathbb{Z}_n.$$

Antes de darmos um exemplo de como o RSA funciona, consideraremos a tabela 4.2 que estabelece a correspondência entre as letras do alfabeto e os números que utilizaremos nas transformações.

Tabela 4.2: Correspondência entre letras e números para o RSA.

a	b	c	d	e	f	g	h	i	j	k	l	m
10	11	12	13	14	15	16	17	18	19	20	21	22
n	o	p	q	r	s	t	u	v	w	x	y	z
23	24	25	26	27	28	29	30	31	32	33	34	35

Iniciamos a partir do número 10 para que não ocorra dúvidas no processo de decifragem. Se utilizássemos aqui a correspondência estabelecida na tabela 2.2 o número 15, por exemplo, poderia representar as letras B e F ou apenas a letra P.

Exemplo:

Mensagem original: `ataque os inimigos`

Chave pública: $n = 221$ e $e = 7$

Transformação:
Inicialmente, escrevemos os números correspondentes das letras da mensagem de acordo com a tabela 4.2:

$$10291026301499242899182318221816242 8.$$

Em seguida, quebramos a mensagem em blocos menores que $n = 221$:

$$102 - 9 - 102 - 6 - 30 - 149 - 92 - 42 - 89 - 91 - 82 - 31 - 82 - 18 - 162 - 42 - 8,$$

e calculamos

$$C = M^7, \ em \ \mathbb{Z}_{221},$$

para cada bloco.
Transformando o primeiro bloco, por exemplo, temos:

$$C(102) = 102^7 = 119, \ em \ \mathbb{Z}_{221}.$$

Procedendo de maneira análoga, ciframos os demais blocos, obtendo:

$$119 - 87 - 119 - 150 - 4 - 72 - 131 - 185 - 132 - 65 - 108 - 125 - 108 - 23 - 189 - 185 - 83.$$

Note que o valor $n = 221$ foi escolhido de forma que $n = pq$, com $p = 13$ e $q = 17$. Além disso, $e = 7$ é tal que $mdc(e, \Phi(221)) = 1$. Satisfazendo assim as condições exigidas pelo RSA.

Para decifrar, precisamos do inverso do número e em $\mathbb{Z}_{\Phi(n)}$.
Como $e = 7$ e $\Phi(n) = \Phi(221) = 12 \cdot 16 = 192$, temos que $d = e^{-1} = 55$, em $\mathbb{Z}_{192}$. Dessa forma, a chave secreta de decifragem será o par $n = 221$ e $d = 55$.
Decifrando o primeiro bloco, obtemos

$$M(119) = 119^{55} = 102, \ em \ \mathbb{Z}_{221}.$$

De maneira análoga, deciframos os demais blocos restabelecendo a mensagem original.

Agora que já observamos o ciframento de uma mensagem pelo RSA, é necessário justificarmos por que $C^d = (M^e)^d = M^{ed} = M$, em $\mathbb{Z}_n$, com $d = e^{-1}$ em $\mathbb{Z}_{\Phi(n)}$.
Acontece que como d é o inverso de e em $\mathbb{Z}_{\Phi(n)}$, temos que

$$ed = 1 + k\Phi(n).$$

Substituindo essa relação em M^{ed}, temos

$$M^{ed} = M^{1+k\Phi(n)} = (M^{\Phi(n)})^k M, \ em \mathbb{Z}_n.$$

Pelo corolário 1.2.2 (teorema de Euler) do teorema de Lagrange, se $mdc(M, n) = 1$, então $M^{\Phi(n)} = 1 \Rightarrow M^{ed} = M$, em $\mathbb{Z}_n$. Mas essa condição nem sempre é satisfeita, como vimos, o bloco M pode assumir qualquer valor de 1 a $n-1$. Dessa forma, devemos encontrar uma outra maneira de demonstrar que $M^{ed} = M$, em $\mathbb{Z}_n$, sem utilizar o teorema de Euler.

Como $ed = 1 + k\Phi(n)$, temos que

$$ed = 1 + k(p-1)(q-1).$$

Considerando $M^{ed} = M^{1+k(p-1)(q-1)} = M(M^{(p-1)})^{k(q-1)}$ em $\mathbb{Z}_p$, e supondo que p não divide M, pelo corolário 1.2.3 (pequeno teorema de Fermat) do teorema de Lagrange, temos que $M^{(p-1)} = 1$ em $\mathbb{Z}_p$, donde $M^{ed} = M$ em $\mathbb{Z}_p$. Por outro lado, se p divide M, então $M = 0$ em $\mathbb{Z}_p$, donde $M^{ed} = M$ em $\mathbb{Z}_p$. Dessa forma, $M^{ed} = M$ em $\mathbb{Z}_p$, para todo inteiro M.

Analogamente, $M^{ed} = M$, em $\mathbb{Z}_q$, para todo inteiro M.

Assim, $M^{ed} - M$ é divisível por p e q. Como p e q são primos distintos e $n = pq$, temos que $M^{ed} - M$ é divisível por n, donde $M^{ed} = M$, em $\mathbb{Z}_n$.

Para finalizar esta seção, ponderaremos alguns aspectos relacionados à segurança do RSA.

Em primeiro lugar, é importante salientar que apesar de termos usado um valor pequeno para n em nosso exemplo, na prática esse parâmetro deve apresentar, aproximadamente, 300 algarismos. Obtém-se n multiplicando dois primos grandes e distintos conforme dissemos ao apresentarmos a relação que permite cifrar uma mensagem.

Observe que como a chave de codificação é de domínio público, a chave de decodificação não pode ser facilmente obtida a partir do seu conhecimento. Em outras palavras, conhecendo-se e e n, deve ser complicado achar $d = e^{-1}$ em $\mathbb{Z}_{\Phi(n)}$.

Considerando a situação com um pouco mais de cuidado, vemos que a única maneira de encontrar $d = e^{-1}$ em $\mathbb{Z}_{\Phi(n)}$, é aplicando o algoritmo euclidiano estendido a $\Phi(n)$ e e. Mas, para isso, é necessário conhecermos os primos p e q que geraram n.

Se n fosse um número pequeno, não haveria obstáculo algum para solucionar essa questão. No entanto, n é um número da ordem de 10^{300}, para o qual não se conhece algoritmo rápido de fatoração. Como afirmamos no capítulo 2, a fatoração de um número dessa grandeza levaria hoje, utilizando um supercomputador, milhares de anos.

É por essa razão que afirmamos no capítulo 2 que a segurança do RSA está relacionada à dificuldade de fatoração de um produto de dois primos grandes.

De qualquer forma, nada nos impede de imaginar que um criptoanalista tenha encontrado uma maneira de chegar a d sem fatorar n.

Suponha, por exemplo, que ele tenha criado um algoritmo rápido de calcular $\Phi(n)$ a partir de n e e. Nesse caso, como conhece n e $\Phi(n)$, pq e $(p-1)(q-1)$ respectivamente, ele pode determinar p e q da seguinte forma:

$$\Phi(n) = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q) + 1$$

$$\Rightarrow p + q = n - \Phi(n) + 1,$$

além disso,

$$(p+q)^2 - 4n = (p-q)^2$$
$$\Rightarrow p - q = \sqrt{(p+q)^2 - 4n}$$

donde p e q são facilmente calculados.

Assim, o criptoanalista, na verdade, teria encontrado uma maneira rápida de fatorar n.

Podemos supor, ainda, que o criptoanalista tenha encontrado uma maneira de chegar a d sem calcular $\Phi(n)$. Dessa forma, como $ed = 1$ em $\mathbb{Z}_{\Phi(n)}$, $ed-1$ é múltiplo de $\Phi(n)$. De acordo com Rosen [18], n poderá ser facilmente fatorado, uma vez que existem algoritmos para fazer isso utilizando um múltiplo de $\Phi(n)$.

Não foi provado que para quebrar o RSA o criptoanalista tem, necessariamente, que fatorar n. Porém, a descoberta de um método que permita quebrar o RSA sem realizar a fatoração de n também parece estar longe.

Nesse sentido, o RSA vem se estabelecendo como um dos sistemas criptográficos mais seguros dentre todos que foram desenvolvidos ao longo da história da criptografia.

Considerações Finais

Como vimos, a evolução da criptografia é marcada pela luta entre criptógrafos e seus oponentes, criptoanalistas. Em outras palavras, cada vez que uma cifra é quebrada pelos criptoanalistas, surge a necessidade de criação de um novo sistema criptográfico, mais complexo, pelos criptógrafos. Nesse sentido, dizemos que a criptoanálise vem contribuindo significativamente para o desenvolvimento da criptografia ao longo da história.

O estudo de alguns dos cripto-sistemas desenvolvidos até então, nos permitiu ter uma idéia de como a álgebra é utilizada na criptografia. Dessa forma, foi possível atingir o objetivo principal desse trabalho.

Vimos também que um grande salto na evolução da criptografia foi dado com a descoberta do RSA. Esse cripto-sistema, além de evitar o transtorno da combinação prévia da chave, se estabeleceu como uma das cifras mais seguras dentre todas as desenvolvidas.

A segurança do RSA apenas estará comprometida, caso criptoanalistas consigam diminuir significativamente o tempo de fatoração de um produto de primos grandes. Fato que pode acontecer caso desenvolvam algoritmos de fatoração rápidos ou o computador quântico.

De qualquer forma, o desenvolvimento tecnológico, que permite a construção de computadores cada vez mais rápidos, impõe a utilização de chaves cada vez maiores. Para se ter uma idéia, quando o RSA foi criado, chaves de 200 algariasmos eram suficientes para garantir a segurança das informações cifradas. Hoje já é necessário utilizar chaves de aproximadamente 300 algarismos.

Nesse sentido, para evitar a utilização de chaves cada vez maiores, já foram desenvolvidos cripto-sistemas de chave pública baseados em curvas elípticas, nos quais aos invés de se usar números inteiros para criptografar, utiliza-se pontos sobre uma curva elíptica.

Referências Bibliográficas

[1] ANDRADE, Lenimar N. *Breve introdução ao Latex.* João Pessoa, UFPB, 2000.

[2] BIANCONI, Ricardo. Um resultado recente: um algoritmo rápido para detectar números primos. *Revista do professor de matemática,* São Paulo, 50: 46 – 47, 2002.

[3] BOLDRINI, José L. e outros. *Álgebra linear.* 3.ed. São Paulo, Harper & Row do Brasil, 1980.

[4] CARVALHO, Maria C. M. (org.) *Construindo o saber.* 9.ed. Campinas, Papirus, 2000.

[5] CHILDS, Lindasay. *A concrete introduction to higer algebra.* New York, Springer-Verlag, 1979.

[6] COSTA, Silvano C. e outros. *Curso de introdução ao Latex.* Piracicaba, USP, 2002.

[7] COUTINHO, Severino C. *Números inteiros e criptografia RSA.* Rio de Janeiro, IMPA, 1997.

[8] DENEEN, Linda L. Secret encryption with public keys. *The UMAP Jounal,* Duluth, 8:9 – 29, 1987.

[9] DENNING, Dorothy E. R. *Cryptogrphy and data security.* Massachusetts, Addison-Wesley, 1982.

[10] FREQÜÊNCIA da ocorrência de letras no português. (2003). *http:// www.numaboa.com.br/criptologia/matematica/estatistica/freqPortBrasil.php*

[11] GALLIAN, Joseph A. *Contemporary abstract algebra.* 4.ed. Boston, Houghton Mifflin Company, 1998.

[12] KOBLITZ, Neal. *A course in number theory and criptography.* New York, Springer-Verlag, 1987.

[13] LANG, Serge. *Undergraduate algebra.* New York, Springer-Verlag, 1987.

[14] LEMOS, Manoel. *Criptografia, números primos e algoritmos.* Rio de Janeiro, IMPA, 2001.

[15] LUCCHESI, Cláudio L. *Introdução à criptografia.* São Paulo, USP, 1984.

[16] MARQUES, Cristina M. *Introdução à teoria de anéis.* Belo Horizonte, UFMG, 2002.

[17] OLIVEIRA, Ivan S. e outros. Computação quântica. *Ciência hoje,* Rio de Janeiro, 33 (193): $22 - 29$, mai. 2003.

[18] ROSEN, Kenneth H. *Elementary number and its applications.* 3.ed. New Jersey, AT&T Bell Laoratories, 1993.

[19] SALOMAA, Arto. *Public-key cryptography.* Berlin Heidelberg, Springer-Verlag, 1990.

[20] SANTOS, Reginaldo J. *Geometria analítica e álgebra linear.* Belo Horizonte, UFMG, 2001.

[21] SANTOS, Reginaldo J. *Introdução ao Latex.* Belo Horizonte, UFMG, 2002.

[22] SEVERINO, A. J. *Metodologia do trabalho científico.* São Paulo, Cortez, 2001.

[23] SINGH, Simon. *O livro dos códigos.* Rio de Janeiro, Record, 2001.

[24] TERADA, Routo. Criptografia e a importância das suas aplicações. *Revista do professor de matemática,* São Paulo, 12: $1 - 7$, 1988.

Créditos das Fotos

Figuras 2.1 e 2.5 ilustrações de Rosilaine de Menezes.
Figuras 2.2, 2.3 e 2.4 Singh [23].
Figuras 3.1 e 3.2 Denning [9].
Figuras 4.1 Salomaa [19].