ESTUDO DE SISTEMAS CRIPTOGRÁFICOS

ADRIELE GIARETTA BIASE* EDSON AGUSTINI†

Resumo

Nesse artigo apresentamos um estudo dos sistemas criptográficos mais comuns em sistemas de comunicações. Além do Sistema Criptográfico RSA, apresentamos os Sistemas ElGamal e Rabin, derivados do RSA. Também apresentamos técnicas de ciframento, como o Criframento de Vigenère, Substituição de Hill, Sistema Merkle-Hellman (MH), Sistema de Rotores e Data Encryption Standard (DES). Para o desenvolvimento desses sistemas criptográficos, introduzimos alguns preliminares de Teoria dos Números, mais precisamente, algoritmos envolvendo números primos e congruências. Procuramos trabalhar com vários exemplos ilustrativos de cada técnica apresentada, com o objetivo de tornar o texto mais compreensivo. Por fim, algumas conclusões são apresentadas.

Palavras-chaves: criptografia, congruência, fatoração, números primos, ciframento.

Abstract

In this article we present a study of some usual cryptosystems in communication systems. Besides RSA Cryptosystem, we present the ElGamal and Rabin Systems, which are arised from the RSA System. We also present some enciphering techniques like Vigenère System, Hill Cryptosystem, Merkle-Hellman (MH) System, Rotor System Machine and Data Encryption Standard (DES). For the development of these cryptosystems, we introduce some prerequisites of Number Theory, more specifically, algorithms about prime numbers and congruencies. We try to work with many appropriated examples of each showed technique, with aim to turn the text more comprehensive. At last, some concluding remarks are presented.

Key-Words: cryptography, congruence, factoring, prime numbers, enciphering.

*Faculdade de Matemática - UFU - Av. João Naves de Ávila, 2121, Uberlândia-MG, 38400-902. E-mail: **adrielegbiase@yahoo.com.br**

†Faculdade de Matemática - UFU - Av. João Naves de Ávila, 2121, Uberlândia - MG, CEP 38400-902. E-mail: **agustini@ufu.br**

1 Introdução

Nas últimas décadas a necessidade de se proteger informações, de modo que alguém indesejável não tenha acesso ao seu conteúdo, tem sido imperiosa. Uma das maneiras de se criar essa desejada proteção para mensagens é a criptografia. O uso corrente da criptografia é encontrado, por exemplo, em transações bancárias via *Internet* ou em compras *on-line* com cartões de crédito. Dessa forma, a criptografia torna-se um agente de segurança em um sistema de comunicações.

A criptografia é um método para codificar (ou modificar) uma mensagem a ser enviada de tal forma que apenas o receptor legítimo consiga interpretá-la. A base da criptografia é a teoria dos números, uma vez que o estudo das propriedades dos números inteiros; mais precisamente, a manipulação de máximos divisores comuns, fatorações, congruências e métodos para determinar números primos são fundamentais para se entender criptografia.

O método mais conhecido de criptografia é o chamado *RSA* (Rivest, Shamir, Adleman) [6] e seus derivados, como o ElGamal e o Rabin [5], aos quais daremos ênfase nesse trabalho. Além desses, há o método DES (Data Encryption Standard) [9] e [4], também abordado nesse trabalho.

Há dois grandes objetivos nesse trabalho. O primeiro consiste no estudo dos principais resultados de Teoria dos Números, principalmente congruências, que são necessários ao estudo de criptografia em geral. O segundo é o estudo de algoritmos das criptografias supracitadas.

Em decorrência do exposto, nosso trabalho está esquematizado em duas grandes partes:

- *Desenvolvimentos Preliminares:* são os principais preliminares da Teoria dos Números e algoritmos necessários à compreensão das criptografias.

- *Resultados:* onde procedemos o ciframento e deciframento de mensagens utilizando criptografias.

2 Materiais e Métodos

Devido ao caráter apenas teórico deste artigo, visando apenas resultados matemáticos, o método empregado foi constituído pelo estudo das referências bibliográficas citadas, discussão da Criptografia *RSA*, resolução de exercícios e verificação da funcionabilidade e segurança das Criptografias: *RSA*, ElGamal, Rabin, Ciframento de Vigenère, Substituição de Hill, MH (Merkle e Hellman), Sistemas de Rotores e o DES.

3 Resultados

3.1 Desenvolvimentos Preliminares

Nessa seção, apresentamos alguns conceitos básicos para o entendimento de métodos de criptografia. Começamos com alguns algoritmos (processos para a resolução de um problema descrito passo a passo), que são bastante úteis para a construção de programas computacionais que visam a resolver um dado problema. Os teoremas e as proposições apresentadas nessa seção são básicas e suas demonstrações podem ser encontradas em livros introdutórios de Teoria dos Números como, por exemplo, [1] e [3].

3.1.1 Teorema de Euclides e Algoritmo Euclidiano

Definimos o *máximo divisor comum* de dois inteiros a e b (a ou b diferente de zero), denotado por mdc (a, b), como sendo o maior inteiro que divide a e b.
O Algoritmo Euclidiano calcula o mdc (máximo divisor comum) de dois números naturais a e b, a partir da aplicação sucessiva do Teorema de Euclides, enunciado e demonstrado abaixo.

Teorema. (*de Euclides*) *Se* $a, b \in \mathbb{N}$ *e* $q, r \in \mathbb{N}$ *tais que* $a = bq + r$, *sendo* $r < b$ *ou* $r = 0$, *então* $\text{mdc}\,(a, b) = \text{mdc}\,(b, r)$.

Demonstração.
Sejam a, b, q, r conforme enunciado. Logo, $a = bq + r$. Sejam:

$$d_1 = \text{mdc}(a, b) \text{ e } d_2 = \text{mdc}(b, r).$$

Queremos mostrar que $d_1 = d_2$.
Primeiro, provaremos que $d_1 \leq d_2$. Como $d_1 = \text{mdc}(a, b)$, então d_1 divide a e d_1 divide b, ou seja, existem inteiros u e v tais que:

$$a = d_1 u \text{ e } b = d_1 v.$$

Substituindo estas expressões para a e b na relação $a = bq + r$, obtemos $d_1 u = d_1 vq + r$, ou seja:

$$r = d_1 u - d_1 vq = d_1(u - vq),$$

ou seja, d_1 divide r. Como d_1 também divide b, então d_1 é um divisor comum de b e r. Mas d_2 é o maior divisor comum entre b e r. Logo, $d_1 \leq d_2$.
De modo análogo, demonstra-se que

$$d_1 \geq d_2.$$

Das duas desiguldades:

$$d_1 \leq d_2 e d_1 \geq d_2,$$

segue que $d_1 = d_2$, ou seja

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

como queríamos.

Algoritmo de Euclides

Procedemos da seguinte maneira para calcular o mdc dos naturais a e b:

$$\begin{aligned}
a &= bq_1 + r_1,\ 0 \leq r_1 < b,\\
b &= r_1 q_2 + r_2,\ 0 \leq r_2 < r_1,\\
r_1 &= r_2 q_3 + r_3,\ 0 \leq r_3 < r_2,\\
r_2 &= r_3 q_4 + r_4,\ 0 \leq r_4 < r_3,\\
&\vdots\\
r_{n-2} &= r_{n-1} q_n + r_n,\ 0 \leq r_n < r_{n-1},
\end{aligned}$$

Esse processo continua até que obtenhamos um $r_n = 0$. Quando isto acontece, temos:

$$\begin{aligned}
\text{mdc}(a, b) &= \text{mdc}\,(b, r_1) = \text{mdc}\,(r_1, r_2) = ...\\
&... = \text{mdc}\,(r_{n-2}, r_{n-1}) =\\
&= \text{mdc}\,(r_{n-1}, 0) = r_{n-1},
\end{aligned}$$

devido ao Teorema de Euclides.

3.1.2 Teorema de Euclides Estendido e Algoritmo Euclidiano Estendido

Proposição 1. *Se $d, n \in \mathbb{Z}^*$ são tais que $d \mid n$, então $|d| \leq |n|$.*

Demonstração.

Temos, pela hipótese:

$$d \mid n \Rightarrow n = kd$$

com $k \in \mathbb{Z}^*$e $n \neq 0$. Logo:

$$n = kd \Rightarrow |n| = |kd| \Rightarrow |n| = |k|\,|d|\,.$$

Suponhamos que $|d| > |n|$. Logo,

$$|d| = |n| + p \text{ com } p \in \mathbb{N}.$$

Assim:

$$|d| = |k|\,|d| + p \Rightarrow (|k| - 1)\,|d| + p = 0.$$

Como $(|k| - 1) \geq 0$ temos $(|k| - 1)\,|d| \geq 0$ e $p > 0$, ou seja,

$$(|k| - 1)\,|d| + p > 0,$$

uma contradição. Logo, $|d| \leq n$, como queríamos.

Teorema (*de Euclides Estendido*) *Sejam $a, b \in \mathbb{N}$ e $d = \text{mdc}\,(a, b)$. Então, existem $\alpha, \beta \in \mathbb{Z}$ tais que:*

$$\alpha a + \beta b = d.$$

Demonstração.
Seja $B = \{na + mb\}$ o conjunto de todas as combinações lineares $na + mb$ sendo n e m inteiros. Escolhemos α e β tais que:

$$c = \alpha a + \beta b$$

seja o menor inteiro positivo pertencente ao conjunto B.
Vamos provar que $c \mid a$ e $c \mid b$. Como as demostrações são análogas, mostremos apenas que $c \mid a$.
Suponhamos que $c \nmid a$. Neste caso pelo Teorema da Divisão de Inteiros, existem q e r tais que $a = qc + r$ com $0 < r < c$. Portanto:

$$\begin{aligned} r &= a - qc = a - q(\alpha a + \beta b) = \\ &= a - q\alpha a - q\beta b = \\ &= (1 - q\alpha)\, a + (-q\beta)\, b. \end{aligned}$$

Como $1 - q\alpha$ e $-q\beta$ são inteiros, então
$r \in B$, o que é uma contradição, uma vez que $0 < r < c$ e c é o menor elemento positivo de B.
Conclusão: $c \mid a$.
De modo similar mostra-se que $c \mid b$.
Como d é um divisor comum de a e b, existem inteiros K_1 e K_2 tais que $a = K_1 d$ e $b = K_2 d$. Portanto,

$$\begin{aligned} &c = \alpha a + \beta b \Rightarrow c = \alpha\,(K_1 d) + \beta\,(K_2 d) \Rightarrow \\ &\quad \Rightarrow c = d\,(\alpha K_1 + \beta K_2)\,. \end{aligned}$$

Logo $d \mid c$. Da Proposição 1 acima, temos que $d \leq c$ (ambos positivos) e como $d < c$ não é possível uma vez que d é o máximo devisor comum. Então $c = d$.
Concluímos então que $d = \alpha a + \beta b$, como queríamos.

Algoritmo Euclidiano Estendido

O algoritmo que fornece d, α e β a partir de a e b é denominado Algoritmo Euclidiano Estendido.
Primeiramente, vamos calcular o $\mathrm{mdc}(a, b)$. Utilizando o Algoritmo Euclidiano, obtemos, a seqüência de divisões abaixo:

$$\begin{aligned} a &= bq_1 + r_1 \text{ e } r_1 = ax_1 + by_1 \\ b &= r_1 q_2 + r_2 \text{ e } r_2 = ax_2 + by_2 \\ r_1 &= r_2 q_3 + r_3 \text{ e } r_3 = ax_3 + by_3 \\ &\vdots \\ r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} \\ &\quad \text{e } r_{n-1} = ax_{n-1} + by_{n-1} \\ r_{n-2} &= r_{n-1} q_n \\ &\quad \text{e } r_n = 0 \end{aligned}$$

Os $x_1, ..., x_{n-1}$ e $y_1, ..., y_{n-1}$ são inteiros a determinar.
Coloquemos os dados obtidos acima em uma tabela:

restos	quocientes	x	y
a	$*$	x_{-1}	y_{-1}
b	$*$	x_0	y_0
r_1	q_1	x_1	y_1
r_2	q_2	x_2	y_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_{n-1}	q_{n-1}	x_{n-1}	y_{n-1}

Embora a e b não sejam restos, as duas primeiras linhas da tabela são convenientes, pois nos ajudam a desenvolver o algoritmo. Sendo assim, iremos chamá-las de linhas -1 e 0.
Vamos desenvolver um algoritmo para determinar as colunas de x e y, utilizando somente duas linhas sucessivas. Para tanto, é necessário imaginar que recebemos a tabela preenchida até um certo ponto: a j-ésima linha, por exemplo. Nessa linha, temos r_{j-2} dividido por r_{j-1}, ou seja,

$$r_{j-2} = r_{j-1} q_j + r_j \Rightarrow r_j = r_{j-2} - r_{j-1} q_j \quad (1)$$

Analisando as duas linhas anteriores: a $(j-1)$-ésima linha e $(j-2)$-ésima linha, encontramos x_{j-1}, y_{j-1}, x_{j-2} e y_{j-2}, sendo:

$$r_{j-1} = ax_{j-1} + by_{j-1} \text{ e } r_{j-2} = ax_{j-2} + by_{j-2}. \quad (2)$$

Substituindo (2) em (1), temos:

$$\begin{aligned} r_j &= ax_{j-2} + by_{j-2} - (ax_{j-1} + by_{j-1})q_j \Rightarrow \\ &\Rightarrow r_j = a(x_{j-2} - x_{j-1}q_j) + \\ &+ b(y_{j-2} - y_{j-1}q_j) \end{aligned}$$

Logo, podemos tomar

$$x_j = x_{j-2} - x_{j-1}q_j \text{ e } y_j = y_{j-2} - y_{j-1}q_j.$$

Temos, portanto, uma fórmula para calcular qualquer x_j e y_j da tabela, utilizando apenas as duas linhas sucessivas $j-2$ e $j-1$ e o quociente da linha j. Para iniciarmos o processo, é necessário ter x_j e y_j de duas linhas sucessivas e é aqui que utilizamos as duas convenientes primeiras linhas:

$$a = ax_{-1} + by_{-1} \text{ e } b = ax_0 + by_0.$$

Nesse caso, os valores triviais para x_{-1}, y_{-1}, x_0 e y_0, são $x_{-1} = 1$, $y_{-1} = 0$, $x_0 = 0$ e $y_0 = 1$. Assim, podemos dar início ao processo e, após executar o algoritmo, tendo descoberto o $d = \text{mdc}\,(a, b)$, ou seja,

$$d = r_{n-1},$$

obtemos:

$$d = r_{n-1} = ax_{n-1} + by_{n-1},$$

ou seja, $\alpha = x_{n-1}$ e $\beta = y_{n-1}$.

3.1.3 O Pequeno Teorema de Fermat

Um resultado bastante útil durante os procedimentos de criptografia e deciframento de mensagens é o teorema enuciado abaixo.

Teorema de Fermat. *Se p é primo e a é um inteiro positivo não divisível por p, então:*

$$a^{p-1} \equiv 1 (\text{mod}\, p).$$

Demostração.
Seja a seqüência de números inteiros positivos entre 1 até $p-1$,

$$1, 2, 3, 4, 5, ..., p-1.$$

Multiplicando cada número dessa seqüencia por a, módulo p, obtem-se o conjunto R de resíduos módulo p, assim determinado:

$$R = \left\{ \begin{array}{c} x_1 \equiv a\,(\text{mod}\, p) \\ x_2 \equiv a\,(\text{mod}\, p) \\ \vdots \\ x_{p-1} \equiv a\,(\text{mod}\, p) \end{array} \right\}$$

Deste modo, $x_1, x_2, ..., x_{p-1}$ são diferentes de zero pois, p não divide a e $x_1, x_2, ..., x_{p-1}$ são distintos. Pois se supormos que

$$x_1 a \equiv x_2 a\,(\text{mod}\, p)\,,$$

onde $1 \leq x_1 < x_2 \leq x_{p-1}$ e, como a é primo com p, podemos eliminar a nos dois lados da congruência, ou seja:

$$x_1 \equiv x_2\,(\text{mod}\, p)\,,$$

o que é absurdo, pois x_1 e x_2 são ambos inteiros positivos menores que p.
Assim, concluimos que os $(p-1)$ elementos de R são todos inteiros positivos, sem que dois elementos sejam iguais.
Portanto, o conjunto R é formado pelo conjunto de inteiros $\{1, 2, 3, ...p-1\}$ em alguma ordem. Multiplicando todas essas congrüências encontramos:

$$\begin{aligned} a.2a.3a...(p-1) &\equiv \\ &\equiv [1.2.3...(p-1)]\,(\text{mod}\, p) \\ &\Rightarrow a^{p-1}\,(p-1)! \equiv \\ &\equiv (p-1)!\,(\text{mod}\, p)\,. \end{aligned}$$

Pelos conceitos da aritmética, podemos cancelar o termo $(p-1)!$ pois ele é relativamente primo de p. Assim,

$$a^{p-1} \equiv 1\,(\text{mod}\, p)\,,$$

como queríamos.

Observação: a congruência $a^p \equiv a\,(\text{mod}\, p)$ é válida quando a é divisível pelo primo p.
De fato, se $\text{mdc}\,(a, p) \neq 1$ e, como p é primo, temos $a = bp$. Logo,

$$a^p - a = b^p p^p - bp = \left(b^p p^{p-1} - b\right) p = kp,$$

ou seja, p divide $a^p - a$, que é equivalente a $a^p - a \equiv 0 \,(\mathrm{mod}\, p)$, que significa

$$a^p \equiv a \,(\mathrm{mod}\, p).$$

Exemplo 1:
Tomando $a = 13$ e $p = 17$ temos:

$$\begin{aligned} 13^2 &\equiv 169 \equiv 16 \,(\mathrm{mod}\, 17) \\ 13^4 &\equiv 2861 \equiv 1 \,(\mathrm{mod}\, 17) \\ 13^8 &\equiv 13^4.13^4 \equiv 1.1 \equiv 1 \,(\mathrm{mod}\, 17) \\ 13^{16} &\equiv 13^8.13^8 \equiv 1.1 \equiv 1 \,(\mathrm{mod}\, 17). \end{aligned}$$

Exemplo 2:
Tomando $p = 3$ e $a = 6$ temos:

$$a^p = 6^3 = 216 \equiv 6 \,(\mathrm{mod}\, 3) \equiv a(\mathrm{mod}\, p).$$

3.1.4 O Teorema de Euler

Outro resultado interessante para criptografia e deciframento é o Teorema de Euler.

A Função ϕ de Euler
Para que possamos estudar o Teorema de Euler é preciso recorrer a alguns pré-requisitos importantes na Teoria dos Números, como a Função ϕ de Euler, denotada por $\phi(n)$, $n \in \mathbb{N}$, e definida como o número de inteiros positivos menores do que n e que são relativamente primos com n. Por convenção, $\phi(1) = 1$, pois $\phi(1)$ não tem significado, mas é definido para que tenha valor 1.

Exemplo 3:
Seja $n = 25$. Temos $\phi(25) = 20$, pois existem vinte números inteiros positivos menores do que 25 relativamente primos com 25. São eles: $1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23$ e 24.

Observemos que para todo número primo p, temos $\phi(p) = p - 1$.

Teorema. *Seja dois números primos p e q, com $p \neq q$. Então, para $n = pq$, temos*

$$\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1).$$

Demonstração.
Para mostrar que $\phi(n) = \phi(p)\phi(q)$, basta considerar todos os números interios positivos menores que n, que é o conjunto $\{1, 2, 3, ..., (pq-1)\}$. Os inteiros nesse conjunto que não são relativamente primos com n são dados pelos conjuntos:

$$\begin{aligned} &\{p, 2p, 3p, ..., (q-1)\,p\} \text{ e} \\ &\{q, 2q, 3q, ..., (p-1)\,q\}. \end{aligned}$$

Assim,

$$\begin{aligned} \phi(n) &= (pq-1) - [(q-1) + (p-1)] \\ &= pq - 1 - q + 1 - p + 1 \\ &= pq - (q+p) + 1 \\ &= (p-1)(q-1) \\ &= \phi(p)\phi(q), \end{aligned}$$

como queríamos.

Teorema de Euler. *Se* $\mathrm{mdc}(a, n) = 1$, *então* $a^{\phi(n)} \equiv 1 \,(\mathrm{mod}\, n)$.

Demonstração.
Considere o conjunto dos números inteiros positivos menores do que n que são relativamente primos com n que denotamos por

$$X = \left\{x_1, x_2, x_3, ..., x_{\phi(n)}\right\}.$$

Deste modo, $\mathrm{mdc}(x_i, n) = 1$, para

$$i = 1, ..., \phi(n).$$

Mutiplicando cada elemento por a, módulo n, temos o conjunto

$$P = \left\{ \begin{array}{c} ax_1 \,(\mathrm{mod}\, n), ax_2 \,(\mathrm{mod}\, n), \\ ax_3 \,(\mathrm{mod}\, n), ..., ax_{\phi(n)} \,(\mathrm{mod}\, n) \end{array} \right\}.$$

Todos os elementos de P são inteiros distintos e relativamente primos com n e menores do que n.
De fato, $ax_i \,(\mathrm{mod}\, n)$ é o resto da divisão de ax_i por n, portanto, $ax_i \,(\mathrm{mod}\, n)$ é menor do que n. Além disso, $\mathrm{mdc}(x_i, n) = 1$ significa que x_i e n não possuem fatores $(\neq 1)$ em comum. Do mesmo modo, como

$\text{mdc}(a,n)=1$, então a e n não possuem fatores ($\neq 1$) em comum. Deste modo, ax_i e n não possuem fatores em comum. Quanto ao fato de serem distintos, temos que se $ax_i \pmod n = ax_j \pmod n$ com $i \neq j$, então $ax_i \equiv ax_j \pmod n$, o que implica

$$x_i \equiv x_j \pmod n,$$

o que não é possível pois

$$x_i \neq x_j \text{ e } x_i, x_j < n.$$

Desta forma,

$$\{x_1, ..., x_{\phi(n)}\}$$

e

$$\left\{ \begin{array}{c} ax_1 \pmod n, ax_2 \pmod n, \\ ax_3 \pmod n, ..., ax_{\phi(n)} \pmod n \end{array} \right\}$$

representam o conjunto de todos os inteiros menores do que n e que são relativamente primos com n. Assim, temos a igualdade entre esses conjuntos e, portanto,

$$\prod_{i=1}^{\phi(n)} (ax_i \pmod n) = \prod_{i=1}^{\phi(n)} x_i \Rightarrow$$

$$\prod_{i=1}^{\phi(n)} ax_i \equiv \left(\prod_{i=1}^{\phi(n)} x_i \right) \pmod n \Rightarrow$$

$$a^{\phi(n)} \left(\prod_{i=1}^{\phi(n)} x_i \right) \equiv \left(\prod_{i=1}^{\phi(n)} x_i \right) \pmod n \Rightarrow$$

$$a^{\phi(n)} \equiv 1 \pmod n,$$

como queríamos.

Observação: a congruência

$$a^{\phi(n)+1} \equiv a \pmod n$$

é válida independente de a ser relativamente primo com n. De fato, decompondo a em fatores primos temos
$a = p_1 p_2 ... p_k$. Logo, pelo Teorema de Euler:

$$\left\{ \begin{array}{l} p_1^{\phi(n)} \equiv 1 \pmod n \Rightarrow p_1^{\phi(n)+1} \equiv p_1 \pmod n \\ p_2^{\phi(n)} \equiv 1 \pmod n \Rightarrow p_2^{\phi(n)+1} \equiv p_2 \pmod n \\ \vdots \\ p_k^{\phi(n)} \equiv 1 \pmod n \Rightarrow p_k^{\phi(n)+1} \equiv p_k \pmod n \end{array} \right.$$

$$\Rightarrow p_1^{\phi(n)+1} p_2^{\phi(n)+1} ... p_k^{\phi(n)+1} \equiv p_1 p_2 ... p_k \pmod n$$

$$\Rightarrow a^{\phi(n)+1} \equiv a \pmod n.$$

Exemplo 4:
Sejam $a = 5$ e $n = 12$. Temos $\phi(12) = 4$ e, portanto,

$$a^{\phi(n)} = 5^4 = 625 \equiv 1 (\text{mod}\, 12) = 1 \pmod n.$$

Sejam $a = 4$ e $n = 15$. Temos $\phi(15) = 8$ e, portanto,

$$a^{\phi(n)} = 4^8 \equiv 1 (\text{mod}\, 15) = 1 \pmod n.$$

3.1.5 O Algoritmo de Miller-Rabin

Não existe um método eficiente para determinar se um número é primo ou composto. Mas existe o algoritmo de Miller-Rabin, que pode auxiliar na determinação destes números. Isto é, dado um número grande primo ao efetuar esse algoritmo, temos uma grande probabilidade de distingui-lo dos números compostos.
O algoritmo de Miller-Rabin é usado para testar se um número grande é primo. Para iniciar a determinação de um número primo ou composto é necessário lembrar que todo número ímpar maior ou igual a 3 pode ser escrito da seguinte forma:

$$n = 2^k q + 1,$$

com $k > 0$, q ímpar onde$(n-1)$ é par.

Algumas propriedades dos números primos:

Proposição 1. *Se p é primo e a é um inteiro positivo menor do que p, então*
$a^2 \equiv 1 \pmod p$ *se, e somente se,*

$$a \equiv 1 \pmod p \;\; \textit{ou}\; a \equiv -1 \pmod p.$$

Demostração.
($\Rightarrow$) Como $1 \equiv a^2 (\text{mod}\, p)$, então

$$1.1 \equiv a.a \pmod p \Rightarrow 1 \equiv a \pmod p^2 \Rightarrow$$

$$\Rightarrow \left\{ \begin{array}{l} a \pmod p \equiv 1 \\ \text{ou} \\ a \pmod p \equiv -1 \end{array} \right. .$$

($\Leftarrow$) Se $1 \equiv a \pmod{p}$, então

$$1.1 \equiv a.a \pmod{p} \Rightarrow 1 \equiv a^2 \pmod{p}.$$

Se $-1 \equiv a \pmod{p}$, então

$$(-1)(-1) \equiv a.a \pmod{p} \Rightarrow 1 \equiv a^2 \pmod{p},$$

como queríamos.

Proposição 2. Seja p um número primo de modo que $p > 2$, então, $p-1 = 2^k q$ para $k > 0$ e que q ímpar. Seja a um número inteiro tal que $1 < a < p-1$. Então:
(i) $a^q \equiv 1 \pmod{p}$.
(ii) Existe algum inteiro j; $1 \leq j \leq k$; tal que $a^{2^{(j-1)}q} \equiv -1 \pmod{p}$.

Demonstração.
Pelo Teorema de Fermat,

$$a^{p-1} \equiv 1 \pmod{n} \text{ se } p \text{ for primo.}$$

Mas,

$$p - 1 = 2^k q.$$

Logo,

$$a^{p-1} \pmod{p} = a^{2^k q} \pmod{p} = 1.$$

Assim, analisando a seqüência de números

$$a^p \pmod{p}, a^{2q} \pmod{p}, a^{4q} \pmod{p}, ...$$
$$..., a^{2^{k-1}q} \pmod{p}, a^{2^k q} \pmod{p}$$

pode-se concluir que o último número da lista tem o valor 1. Deste modo, cada número na lista é o quadrado do número anterior. Logo, existem duas possibilidades:
(1) Por (i) temos que o primeiro número da lista e, conseqüentemente, todos os números subseqüentes na lista, é igual a 1.
(2) Por (ii) algum número na lista não será igual a 1, mas o seu quadrado $\bmod p$ será igual a 1. E o único número que satisfaz essa condição é $p-1$. Logo, em toda lista existe um elemento igual a $p-1$.
Com isto, concluímos a demonstração.

Observação: As considerações feitas anteriormente leva à seguinte situação: se n for primo, então ou o primeiro elemento da lista de resíduos $\left(a^q, a^{2q}, ..., a^{2^{(k-1)}q}, a^{2^k q}\right) \pmod{n}$ é igual a 1, ou algum elemento na lista é igual a $n-1$.
Caso essa situação não ocorra, n é composto, ou seja, não é primo. Porém, caso a situação ocorrer, ainda não podemos afirmar que n é primo. E, neste caso, o algoritmo retornará com o resultado: INCONCLUSIVO.

Exemplo 5:
Para $n = 2047$, então,

$$n - 1 = 2.1023.$$

Calculando:

$$2^{1023} \pmod{2047} \equiv 1.$$

O número 2047 atende a condição, mas é um número composto, pois $2047 = 23.84$, portanto, não se chega a conclusão de que o número é primo.

Algoritmo de Miller-Rabin

1^a Etapa) Escolha inteiros k, q com $k > 0$ e q ímpar, de modo que $(n-1) = 2^k q$;
2^a Etapa) Escolha um inteiro aleatório a, de modo que pertença ao intervalo
$1 < a < n-1$;
3^a Etapa) Se $a^q \pmod{n} \equiv 1$, então escreva INCONCLUSIVO;
4^a Etapa) Para $j = 0$ até $k-1$ faça:
Se $a^{2^j q} \pmod{n} \equiv n-1$, então escreva INCONCLUSIVO. Caso contrário, escreva COMPOSTO.

3.1.6 Método dos Quadrados Repetidos

O objetivo desse método é calcular a congruência de $b^r \pmod{n}$, sendo b, r e n números naturais grandes.
Para fazer esse cálculo, é necessário convertermos r em número binário. Para tanto, suponhamos

$$r = \sum_{j=0}^{k} a_j 2^j,$$

sendo $a_j = 0$ ou 1.

Algoritmo:
Sejam c, d e b_j; $j = 0, ..., k$; números naturais (auxiliares).

Passo 1) Se $a_0 = 1$, então faça $c = b$. Senão, faça $c = 1$.

Passo 2) Seja $b_0 = b$.

Passo 3) Para cada $j = 1, ..., k$ faça:
Calcule $b_j \equiv b_{j-1}^2 \pmod{n}$.
Se $a_j = 1$, calcule

$$d \equiv cb_j \pmod{n}$$

e faça $c = d$. Senão deixe c inalterado.

Passo 4) O número c é côngruo a b^r módulo n, ou seja, $c \equiv b^r \pmod{n}$.

Percebemos que na etapa i do Passo 3, temos $c \equiv b_0^{\sum_{j=0}^{i} a_j 2^j} \pmod{n}$. Assim, ao término do algoritmo, temos

$$c \equiv b^r \pmod{n}.$$

Exemplo 6:
Calculemos $b^r \pmod{n}$, onde

$$b = 227, r = 106 \text{ e } n = 451.$$

Passando $r = 106$ para a base binária, temos:

$$106 = 1101010 =$$
$$= (0.2^0 + 1.2^1 + 0.2^2 + 1.2^3 +$$
$$+0.2^4 + 1.2^5 + 1.2^6).$$

Logo, $k = 6$, e $a_0 = 0$, $a_1 = 1$, $a_2 = 0$, $a_3 = 1$, $a_4 = 0$, $a_5 = 1$ e $a_6 = 1$. Seguindo o algoritmo:

Passo 1) Como $a_0 \neq 1$, então $c = 1$.

Passo 2) $b_0 = 227$.

Passo 3)

Para $j = 1$
$b_1 \equiv 227^2 \pmod{451} \Rightarrow b_1 = 115$
$a_0 \equiv 1$, então $d \equiv 1.115 (\mathrm{mod}\, 451) \Rightarrow$
$\Rightarrow d = 115 \Rightarrow c = 115$
Para $j = 2$
$b_2 \equiv 115^2 \pmod{451} \Rightarrow b_2 = 146$
$a_2 = 0 \Rightarrow c = 115$
Para $j = 3$
$b_3 \equiv 146^2 (\mathrm{mod}\, 451) \Rightarrow b_3 = 119$
$a_3 = 1$, então $d \equiv 115.119 (\mathrm{mod}\, 451) \Rightarrow$
$\Rightarrow d = 20 \Rightarrow c = 20$
Para $j = 4$
$b_4 \equiv 119^2 (\mathrm{mod}\, 451) \Rightarrow b_4 = 180$
$a_4 = 0 \Rightarrow c = 20$
Para $j = 5$
$b_5 \equiv 180^2 (\mathrm{mod}\, 451) \Rightarrow b_5 = 379$
$a_0 = 1 \Rightarrow d \equiv 20.379 (\mathrm{mod}\, 451) \Rightarrow$
$\Rightarrow d = 364 \Rightarrow c = 364$
Para $j = 6$
$b_6 \equiv 379^2 (\mathrm{mod}\, 451) \Rightarrow b_6 = 223$
$a_6 = 1 \Rightarrow d \equiv 364.223 (\mathrm{mod}\, 451) \Rightarrow$
$d = 443 \Rightarrow c = 443$

Passo 4) Logo,

$$b^r \pmod{n} = 443 \equiv 227^{106} (\mathrm{mod}\, 451).$$

3.2 Criptografias

Para criptografar devemos converter uma mensagem em uma seqüência de números. Para efeito de exemplificação, tomemos a seguinte tabela de conversão:

a	b	c	d	e	f	g	h	i
10	11	12	13	14	15	16	17	18

j	k	l	m	n	o	p	q	r
19	20	21	22	23	24	25	26	27

s	t	u	v	w	x	y	z	_
28	29	30	31	32	33	34	35	36

0	1	2	3	4	5	6	7	8	9
37	38	39	40	41	42	43	44	45	46

Tabela 1

O espaço entre palavras será substituído pelo n^o. 36. As conversões do texto a ser

cifrado será feito sem considerar acentos e letras maiúscula. A vantagem de se utilizar 2 dígitos para representar uma letra reside no fato de que tal procedimento evita a ocorrência de ambigüidades. Por exemplo, se a fosse convertido em 1 e b em 2, teríamos que ab seria 12, mas l também seria 12. Logo, não poderíamos concluir se 12 seria ab ou l.

3.2.1 Criptografia RSA

Pré-Codificação Para usarmos o método *RSA,* devemos converter uma mensagem em uma seqüência de números. Chamaremos essa etapa de *pré-codificação.*
Para efeito de exemplificação, tomemos a tabela de conversão dada anteriormemte para realizar a fase de pré-codificação. Assim a frase "$Famat\_2008$"[1], é convertida no número

$$15102210293639373745$$

Precisamos determinar 2 primos distintos, que denotaremos por p e q, que são denominados *parâmetros RSA.* Seja

$$n = pq,$$

que é chamado de *módulo RSA.*
A última etapa da pré-codificação consiste em separar o número acima em blocos cujos valores sejam menores que n.
A mensagem cuja conversão foi feita acima pode ser separada nos seguintes blocos:

$$15\ 10\ 22\ 10\ 29\ 36\ 39\ 37\ 37\ 45.$$

A maneira de escolher os blocos não é única e não precisa ser homogênea (todos os blocos com o mesmo número de dígitos), mas devemos tomar alguns cuidados como, por exemplo, não começar um bloco com zero, pois isto traria problemas na hora de montar a seqüência recebida (o zero no início do bloco pode não aparecer!).

[1]Faremos a conversão sem considerar acentos e letras maiúsculas.

Codificação e Decodificação Passemos ao processo de codificação. Da subseção acima, temos $n = pq$ com p e q primos. Tomemos a Função ϕ de Euler:

$$\phi(n) = (p-1)(q-1).$$

Seja $e < \phi(n)$ inteiro positivo inversível módulo $\phi(n)$, ou seja,

$$\text{mdc}(e, \phi(n)) = 1.$$

Esse número e é chamado de *expoente de enciframento.*
O par (n, e) é denominado *chave pública de codificação do sistema RSA.*
Agora, codifiquemos cada bloco obtido na pré-codificação (subseção anterior). Após a codificação, os blocos não poderão ser reunidos de modo que não possamos distinguí-los, pois isto tornaria impossível a decodificação da mensagem.
A codificação de um bloco b será denotada por $C(b)$. Temos que $C(b)$ é o resto da divisão de b^e por n, isto é,

$$C(b) \equiv b^e \pmod{n}.$$

Por exemplo, se $p = 29$ e $q = 67$, então $n = 1943$. Logo, $\phi(n) = 1848$. Tomemos $e = 701$ (observe que $\text{mdc}(701, 1848) = 1$). Assim, o último bloco, 45, da mensagem anterior é codificado como o resto da divisão de 45^{701} por 1943. Convertendo 701 em binário e utilizando o método dos quadrados repetidos, temos

$$161 \equiv 45^{701} \pmod{1943}.$$

Codificando toda a mensagem, obtemos a seguinte seqüência de blocos:

$$595\ 155\ 1842\ 155\ 841$$
$$384\ 1344\ 1168\ 1168\ 161.$$

Para decodificar uma mensagem codificada, precisamos de n e do inverso de e módulo $\phi(n)$, que chamaremos de d, ou seja

$$ed \equiv 1 \pmod{\phi(n)}.$$

O par (n, d) é denominado *chave privada de decodificação do sistema RSA.*
Seja $a = C(b)$ um bloco da mensagem codificada, então $D(a)$ será o resultado da decodificação. Temos que $D(a)$ é o resto da divisão de a^d por n, isto é,

$$D(a) \equiv a^d \pmod{n}.$$

Esperamos que, decodificando os blocos da mensagem codificada, possamos encontrar a mensagem original, ou seja, $D(C(b)) = b$. Para decodificarmos, não é necessário conhecermos p e q, basta conhecer n e d.
No exemplo que estamos acompanhando, temos que $n = 1943$ e $e = 701$.
Usando o algoritmo euclidiano estendido, temos $d = 29$.
Assim, para decodificar o bloco 161 recebido, devemos calcular o resto da divisão de 1317^{29} por 1943 (utilizando, por exemplo, o *Método dos Quadrados Repetidos*), ou seja, 45:

$$45 \equiv 161^{29} \pmod{1943}.$$

Logo, a seqüência decodificada será

$$15\ 10\ 22\ 10\ 29\ 36\ 39\ 37\ 37\ 45,$$

que corresponde, via tabela de conversão, à frase "$Famat\_2008$".
Observação:
Pode ocorrer que no cálculo de d encontremos um valor negativo. No entanto, é sempre possível tomar um valor positivo de d utilizando o teorema da solução geral de uma equação diofantina.
Vejamos um exemplo com $p = 31$ e $q = 47$.
Na codificação:

$$\phi(n) = (p-1)(q-1) = 30.46 = 1380$$
$$n = pq = 31.47 = 1457$$

Se tomarmos $e = 1001$ (pois temos $\text{mdc}(1001, 1380) = 1$) e o primeiro bloco da mensagem anterior, cujo o número associado é 15, então a decodificação desta mensagem será o resto da divisão de 15^{1001} por 1457. Convertendo 1001 em um binário e utilizando o *Método dos Quadrados Repetidos*, temos:

$$C(b) \equiv 15^{1001} \pmod{1457}$$
$$1100 \equiv 15^{1001} \pmod{1457}$$

Na decodificação:
O par (n, d) é a chave privada da decodificação do sistema RSA. Seja $a = C(a)$ a mensagem codificada, então $D(a)$ será o resultado da decodificação. Mas temos que $D(a)$ é o resto da divisão de a^d por n, ou seja:

$$D(a) \equiv a^d \pmod{n}.$$

Calculemos o valor de d a partir do *Algoritmo Euclidiano Estendido*, pois:

$$1 = \phi(n)\, k - ed.$$

Usando uma tabela:

i	Restos	Quocientes	x_i	y_i
-1	1380	$*$	1	0
0	1001	$*$	0	1
1	379	1	1	-1
2	243	2	-2	3
3	136	1	3	-4
4	107	1	-5	7
5	29	1	8	-11
6	20	3	-29	40
7	9	1	37	-51
8	2	2	-103	142
9	1	4	449	-619
	0	2		

Temos

$$d = y_9 = -619.$$

Mas não nos interessa trabalhar com valores de d negativos, para isso temos o algoritmo derivado do teorema da solução geral de uma equação diofantina que encontra um valor positivo para d.

Algoritmo Para Reverter Valores de d Negativos

Etapa 1) Calcular o valor de d normalmente.

Etapa 2) Se $d < 0$, então faça
$\overline{d} = d + \phi(n)t$ para t inteiro de tal modo que $\overline{d} > 0$.
Etapa 3) Faça $d = \overline{d}$.

Logo, para o nosso exemplo anterior:

$$\overline{d} = -619 + 1380t, \text{ para } t = 1$$
$$\overline{d} = 1380 - 619$$
$$\overline{d} = 761$$
$$d = \overline{d} = 761$$

Deste modo, após encontrar o novo valor de d (positivo), então continua-se a decodificação usando o *Algoritmo dos Quadrados Repetidos*. Como $D(C(b)) = b$ e para decodificar não é necessario conhecer os valores de p e q, então basta conhecer n e d. Assim, se $n = 1457$ e $e = 1001$, basta resolver a equação:

$$D(a) \equiv 1100^{761} \pmod{1457}$$

no qual devemos obter

$$15 \equiv 1100^{761} \pmod{1457}.$$

No qual era o resultado esperado, nesta decodificação, que era a mensagem inicial.

3.2.2 A Criptografia Rabin

À semelhança da Criptografia RSA, temos que determinar duas chaves para a criptografia Rabin: uma pública e outra privada.

Geração das Chaves na Criptografia Rabin
Na geração das chaves pública e privada da Criptografia Rabin, temos que:

- Escolher dois números primos p e q distintos e grandes de maneira que p seja *próximo* de q e $p \equiv q \equiv 3 \pmod{4}$.
- Calcular $n = pq$.
- A chave pública (número que deve ser divulgado para o emissor A) é n e a chave privada (números que são mantidos em sigilo pelo receptor B) é (p, q).

Etapa de Ciframento
Nesta etapa o emissor A deverá:

- Obter a chave pública n do receptor B.
- Converter as letras, números e símbolos da mensagem em números m entre 0 e $n - 1$. (exemplo: supondo $n > 46$, a Tabela 1 pode ser utilizada)
- Para cada número m, obtido nas conversões acima, calcular $c \equiv m^2 \pmod{n}$.
- Enviar a mensagem cifrada composta pelos números c dos cálculos acima para o receptor B.

Etapa de Deciframento
Uma vez que o receptor B recebe a mensagem cifrada composta pelos números c, então ele deverá:

- Encontrar as quatro raízes quadradas m_j com $j = 1, 2, 3, 4$ de c módulo n.
- O número m, na mensagem original, é um dos m_j.

O receptor B deve determinar qual das quatro possibilidades para os m_j é a mensagem enviada. Se a mensagem é um texto literário, então a tarefa é fácil, pois apenas um dos m_j fará sentido. Entretanto, se o texto não for composto por palavras de um idioma, como por exemplo, uma seqüência aleatória de números e letras, então pode não ser tão fácil determinar o m_j correto.

Uma maneira para superar este problema é acrescentar redundâncias binárias na mensagem original convertida para a base binária. Para isto, basta repetir uma quantidade fixa de dígitos no final da mensagem. Assim, o m_j correto irá reproduzir essas redundâncias, enquanto que é altamente improvável que uma das três outras raízes quadradas m_j venha a reproduzir essas redundâncias. Portanto,

o receptor B pode escolher corretamente a mensagem enviada.
A demonstração da funcionalidade da Criptografia Rabin pode ser encontrada em [5].
Antes de apresentarmos um exemplo, enunciaremos a proposição que fornece as quatro raízes quadradas de a módulo $n = pq$, para certos p e q, utilizadas na etapa de decifra-mento.

Proposição 3. *Seja* $a \in \mathbb{N}$ *e*

$$a \equiv z^2 \,(\mathrm{mod}\, pq)$$

onde p *e* q *são primos e*

$$p \equiv q \equiv 3 \,(\mathrm{mod}\, 4)\,,$$

então existe somente quatro raízes quadradas de a *módulo* pq *e elas são dadas a seguir:*

$$z = \pm xpa^{\frac{q+1}{4}} + yq^{\frac{p+1}{4}}$$

e

$$z = \pm xpa^{\frac{q+1}{4}} - yq^{\frac{p+1}{4}}$$

sendo que $x, y \in \mathbb{Z}$*, podem ser obtidos pelo Algoritmo de Euclides Estendido de modo que*

$$xp + yq = 1.$$

Exemplo 7:
Seja $FAMAT\_2008$ a mensagem a ser cifrada, tomemos $p = 179$ e $q = 43$ e $n = pq = 7697$.- Então, n é a chave pública e $(179, 43)$ é a chave privada. Vamos criptografar a letra M da $FAMAT$. Se utilizarmos a Tabela 1, M corresponde ao $m = 22$.
Representando 22 na base binária:

$$0.2^0 + 1.2^1 + 1.2^2 + 0.2^3 + 1.2^4,$$

então $m = 10110$. Vamos introduzir redundâncias repetindo os quatro últimos digitos, ou seja, temos

$$m' = 101100110,$$

que equivale ao 358 em decimal. Então:

$$\begin{aligned} c &\equiv (m')^2 \,(\mathrm{mod}\, 7697) \Rightarrow \\ &\Rightarrow c \equiv 128164 \,(\mathrm{mod}\, 7697) \Rightarrow \\ &\Rightarrow c = 5012 \end{aligned}$$

e c é enviado ao receptor.
Para decifrar, precisamos de encontrar as quatros raízes quadradas de $c = 5012$ módulo 7697. Utilizando a proposição temos:
Pelo *Algoritmo de Euclides Estendido* encontramos x e y de modo que:

$$xp + yq = 1,$$

que, neste caso corresponde a:

$$(-6)\,(179) + (25)\,(43) = 1,$$

ou seja, $x = -6$ e $y = 25$.
Como $c = 5012$, temos

$$\begin{aligned} m_1 &\equiv \left(-1074.5012^{11} + 1075.5012^{45}\right) (\mathrm{mod}\, 7697) \\ m_2 &\equiv -\left(-1074.5012^{11} + 1075.5012^{45}\right) (\mathrm{mod}\, 7697) \\ m_3 &\equiv \left(1074.5012^{11} - 1075.5012^{45}\right) (\mathrm{mod}\, 7697) \\ m_4 &\equiv -\left(1074.5012^{11} - 1075.5012^{45}\right) (\mathrm{mod}\, 7697) \end{aligned}$$

Usando o Método dos Quadrados Repetidos, segue que:

$$\begin{aligned} 358 &\equiv 5012^{11} \,(\mathrm{mod}\, 7697) \\ 537 &\equiv 5012^{45} \,(\mathrm{mod}\, 7697)\,. \end{aligned}$$

Logo,

$$\begin{aligned} m_1 &\equiv (-1074.358 + 1075.537) \equiv 358 \,(\mathrm{mod}\, 7697) \\ m_2 &\equiv -358 \equiv 7339 \,(\mathrm{mod}\, 7339) \\ m_3 &\equiv (1074.358 - 1075.537) \equiv 7339 \,(\mathrm{mod}\, 7697) \\ m_4 &\equiv -7339 \equiv 358 \,(\mathrm{mod}\, 7697) \end{aligned}$$

ou seja,

$$m_1 = m_4 = 358 \text{ e } m_2 = m_3 = 7339.$$

Suas representações binárias são:

$$\begin{aligned} m_2 = m_3 &= 1110010101011 \\ m_1 = m_4 &= 101100110 \end{aligned}$$

Logo, duas raízes apresentaram redundâncias: m_1 e m_4. Mas $m_1 = m_4$ e, tirando as redundâncias dessas raízes e passando para a base decimal, voltamos para a mensagem original, ou seja, o número 22 que corresponde à letra M.

3.2.3 A Criptografia ElGamal

A Geração de Chaves na Criptografia ElGamal

Na geração das chaves da Criptografia ElGamal, temos que:

- Escolher um número primo grande p e um gerador α do grupo multiplicativo $\mathbb{Z}_p^*$.
- Selecionar ao acaso um número natural $a < p-1$ e calcular $\alpha^a \pmod p$.
- A chave pública é (p, α, α^a) e a chave privada é a.

Etapa de Ciframento

Nesta etapa o emissor A deverá:

- Obter a chave pública (p, α, α^a) de B.
- Converter as letras, números e símbolos da mensagem um números m entre 0 e $p-1$. (exemplo: supondo $p > 46$, a Tabela 1 pode ser utilizada)
- Escolher ao acaso um número natural b, tal que $b < p-1$.
- Para cada m obtido acima, calcular

$$\beta \equiv \alpha^b \pmod p$$
$$\gamma \equiv m\,(\alpha^a)^b \pmod p$$

- Enviar o ciframento $c = (\beta, \gamma)$ de m para B.

Etapa de Deciframento

Uma vez que o receptor B recebe a mensagem cifrada c, então deverá:

- Usar a chave privada para calcular

$$\beta^{p-1-a} \pmod p.$$

- Decifrar m calculando $\beta^{-a}\gamma \pmod p$.
- Temos

$$\beta^{-a}\gamma \equiv \alpha^{-ab} m \alpha^{ab} \equiv m \pmod p$$

devido ao *Teorema de Fermat*.

A demonstração da funcionalidade da Criptografia ElGamal pode ser encontrada em [5].

Exemplo 8:

Seja a frase $FAMAT\_2008$. Tomando $p = 1999$ e escolhendo um gerador $\alpha = 7$ de $\mathbb{Z}_{1999}^*$. O destinatário B escolhe a chave privada $a = 117$.

Usando a Criptografia ElGamal vamos fazer o ciframento e deciframento da letra M da mensagem, que corresponde a $m = 22$ na Tabela 1. Suponha que o emissor A escolha $b = 503$. Para cifrar o emissor A, deve calcular

$$\alpha^a \pmod p = 7^{117} \pmod{1999}.$$

Usando o *Algoritmo dos Quadrados Repetidos*, encontramos $\alpha^a = 54$.
Depois calculamos

$$\beta \equiv \alpha^b \pmod p = 7^{503} \pmod{1999}.$$

Usando o *Algoritmo dos Quadrados Repetidos*, encontramos $\beta = 300$.
Em seguida calculamos

$$\gamma \equiv m\,(\alpha^a)^b \pmod p = 22\,(54)^{503} \pmod{1999}.$$

Usando também o *Algoritmo dos Quadrados Repetidos*, encontramos $\gamma = 77$.
Logo, A envia $(\beta, \gamma) = (300, 77)$ para B.

Para decifrar, B deve:
Calcular

$$\begin{aligned}\beta^{p-1-a} &= 300^{1999-1-117} \pmod{1999} \\ &= 300^{1881} \pmod{1999}.\end{aligned}$$

Usando o *Algoritmo dos Quadrados Repetidos*, encontramos $\beta^{p-1-a} = 857$.
Finalmente, B calcula m, de modo que:

$$m = \beta^{-a}\gamma \equiv 857 \times 77 \pmod{1999}.$$

Ao resolver a congruência acima, encontramos $m = 22$, o que corresponde à letra M da mensagem inicial enviada.

3.2.4 Algumas Técnicas de Cifra-mento

Alguns algoritmos de ciframento fazem uso de três técnicas: transposições, substituições e ciframentos compostos.

Transposições Essa técnica de ciframento consiste simplesmente em uma mudança nas letras da mensagem a ser enviada, de acordo com um critério fixo estabelecido.

Exemplo 9:
Suponha que a mensagem seja dividida em blocos de 5 letras e que, em cada um desses blocos, as letras sejam misturadas de acordo com uma permutação, previamente estabelecida. Suponha que esta permutação seja dada por:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix}.$$

Temos então:
Texto: $FAMAT\_2008$.
Texto dividido em blocos de 5 letras: $FAMAT$ $\_2008$.
Texto cifrado: $MFAAT$ 0_028.
Esse tipo de técnica de ciframento não é aconselhavél, pois a frequência das letras apresentadas no texto cifrado é igual a freqüência das letras do texto original. Quanto menor o bloco mais fácil de descobrir o ordenamento quebrando esse sistema de ciframento.

Substituições Nessa técnica de ciframento ocorre apenas a substituição dos símbolos do texto original por outros (ou por números, de acordo com um algoritmo ou uma tabela como, por exemplo, a Tabela 1) mantendo a posição dos símbolos do texto original.
A substituição pode ser monoafabética ou polialfabética. No primeiro caso, símbolos iguais da mensagem original são sempre substituídos por um mesmo símbolo. Por exemplo, toda letra A é sempre substituída pela letra T. No segundo caso, símbolos iguais da mensagem original podem ser substituídos por símbolos diferentes. Por exemplo, uma letra A da mensagem é substituída pela letra Z e uma outra letra A é substituída pela letra J.
Substituições monoalfabéticas não são técnicas muito eficientes, pois textos literários cifrados com essa técnica podem ser facilmente decifrados. Isso se deve ao fato de que a freqüencia média com que cada letra é usada em uma língua é mais ou menos constante. Por exemplo, na língua portuguesa, as vogais são mais usadas que as consoantes sendo que a vogal a aparece com mais freqüência. Temos ainda que, quando se tem monossílabo no texto, a probalilidade de ser vogal é maior. Por fim, as consoantes s e m aparecem com mais frenqüência.

Exemplo 10: Substituindo símbolos por números.
Tomemos o texto $FAMAT\_2008$. Utilizando a Tabela 1, temos o texto cifrado

15 10 22 10 29 36 39 37 37 45.

Exemplo 11: *O Ciframento de César.* Substituindo símbolo por símbolo.
O Ciframento de César de ordem k é uma substituição monoalfabética que consiste em trocar um símbolo da mensagem original pelo símbolo que está k posições depois do símbolo que se deseja trocar.
Por exemplo, se $k = 2$, então $FAMAT\_2008$ é substituída por $HCOCV1422A$.
A ordem com que as letras são posicionadas é a usual, ou seja:

$$ABCDEFGHIJKLMNOPQRSTU$$
$$VWXYZ\_0123456789ABCDE...$$

Ciframentos Compostos O ciframento composto é monoafabético e é obtido por uma mistura das técnicas de transposição e substituição, isto é depende da letra original e também da sua posição no texto.
Mesmo que o ciframento composto seja formado de substituições e transposições, este

sistema ainda não é seguro. Para um texto grande a dificuldade de quebrar o sistema é maior, mas se o texto for pequeno, essa técnica de ciframento torna-se fácil de ser decifrada.

Exemplo 12:
Vamos supor que o texto original seja dividido em blocos de comprimento 7, como na técnica de transposição, sendo a permutação dada por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 5 & 2 & 1 & 6 & 4 \end{pmatrix}.$$

Caso seja necessário, completamos o último bloco com espaços em branco, representados pelo símbolo _.
Além da permutação σ, vamos usar também a técnica de substituição, de acordo com a TABELA 1.
Temos então:
Texto: $FAMAT\_2008$.
Texto dividido em blocos de 7 letras: $FAMAT\_2 \quad 008\_ \_ \_ \_$.
Texto permutado:

$$2MTAF\_A \quad \_8\_00\_\_.$$

Texto cifrado:

39 22 29 10 15 36 10
36 45 36 37 37 36 36.

3.2.5 Criptografia por Substituição de Hill

A Substituição de Hill é polialfabética e assimétrica, ou seja, o algoritmo de ciframento é diferente do algoritmo de deciframento. Neste sistema criptográfico escolhemos um valor n, por exemplo $n = 3$. Dividimos o texto em blocos de 3 letras, completando o último bloco, caso seja necessário, com espaços em branco, representados pelo símbolo _. Ilustraremos esse método por meio de um exemplo.

Exemplo 13:
Texto: $FAMAT\_2008$.

Etapa de ciframento:
Vamos dividir o texto em blocos de 3 letras: $FAM \quad AT\_ \quad 200 \quad 8\_\_$.
A cada letra dos blocos devemos associar os números correspondentes entre 10 e 46 de acordo com uma tabela de substituição como, por exemplo, a TABELA 1. Assim, obtemos o equivalente numérico ao texto:

15 10 22 10 29 36 39 37 37 45 36 36.

Escolhemos uma matriz $T_{n\times n}$, cujos coeficientes sejam todos inteiros e de modo que $\text{mdc}(\det T, k) = 1$, no qual k é a quantidade de substituições possíveis de acordo com a TABELA 1 que, neste caso, é $k = 37$.
Por exemplo, tomemos a matriz

$$T = \begin{bmatrix} 5 & 11 & 0 \\ 9 & 1 & 3 \\ 17 & 4 & 2 \end{bmatrix}.$$

Assim,

$$\text{mdc}(\det T, k) = \text{mdc}(313, 37) = 1.$$

Vamos considerar cada um dos n blocos do texto como sendo um vetor t_i; $i = 1, ..., n$; em $\mathbb{Z}_{37}^3$ e cifrar o vetor t_i pelo resultado do produto matricial $c_i = T.t_i \,(\text{mod}\, 37)$. Continuando o exemplo, temos:
Para t_1:

$$c_1 = \begin{bmatrix} 5 & 11 & 0 \\ 9 & 1 & 3 \\ 17 & 4 & 2 \end{bmatrix} \begin{bmatrix} 15 \\ 10 \\ 22 \end{bmatrix} (\text{mod}\, 37) = \\ = \begin{bmatrix} 0 \\ 26 \\ 6 \end{bmatrix}.$$

Para t_2:

$$c_2 = \begin{bmatrix} 5 & 11 & 0 \\ 9 & 1 & 3 \\ 17 & 4 & 2 \end{bmatrix} \begin{bmatrix} 10 \\ 29 \\ 36 \end{bmatrix} (\text{mod}\, 37) = \\ = \begin{bmatrix} 36 \\ 5 \\ 25 \end{bmatrix}.$$

Para t_3:

$$c_3 = \begin{bmatrix} 5 & 11 & 0 \\ 9 & 1 & 3 \\ 17 & 4 & 2 \end{bmatrix} \begin{bmatrix} 39 \\ 37 \\ 37 \end{bmatrix} (\text{mod}\, 37) = \\ = \begin{bmatrix} 10 \\ 18 \\ 34 \end{bmatrix}.$$

Para t_4:

$$c_4 = \begin{bmatrix} 5 & 11 & 0 \\ 9 & 1 & 3 \\ 17 & 4 & 2 \end{bmatrix} \begin{bmatrix} 45 \\ 36 \\ 36 \end{bmatrix} (\text{mod}\, 37) = \\ = \begin{bmatrix} 29 \\ 31 \\ 19 \end{bmatrix}.$$

O texto cifrado é constituído pelos blocos c_1, c_2, c_3 e c_4. No exemplo:

$$0\ 26\ 6\ 36\ 5\ 25\ 10\ 18\ 34\ 29\ 31\ 19.$$

Etapa de deciframento
Para decifrar o texto temos que calcular o produto matricial $T^{-1}.c_i\,(\text{mod}\, 37)$.
O cálculo da matriz inversa $T^{-1}\,(\text{mod}\, 37)$ pode ser feito de acordo com o seguinte roteiro:
(1) Achar a inversa de T (sem congruências); No exemplo, temos que a inversa de T é: $\frac{1}{313}\begin{bmatrix} -10 & -22 & 33 \\ 33 & 10 & -15 \\ 19 & 167 & -94 \end{bmatrix}$.
(2) Na matriz inversa encontrada acima, temos na primeira entrada $a_{11} = \frac{a}{d}$;
Precisamos de

$$b \equiv \frac{a}{d}\,(\text{mod}\, 37) \Leftrightarrow \\ bd \equiv a\,(\text{mod}\, 37) \Leftrightarrow \\ bd - a \equiv 0\,(\text{mod}\, 37) \Leftrightarrow \\ bd - a = 37k,$$

onde $k \in \mathbb{Z}$.
No exemplo temos $a_{11} = \frac{-10}{313}$. Assim, $b.313 + 10 = 37k$, que terá solução quando $b = 19$, que, neste caso, corresponde a $k = 161$.

Fazendo o procedimento análogo para cada entrada da matriz, teremos que $T^{-1}\,(\text{mod}\ 37)$ é:

$$\begin{bmatrix} 19 & 27 & 15 \\ 15 & 18 & 10 \\ 12 & 12 & 1 \end{bmatrix}.$$

e, portanto,

$$\begin{bmatrix} 5 & 11 & 0 \\ 9 & 1 & 3 \\ 17 & 4 & 2 \end{bmatrix}.\begin{bmatrix} 19 & 27 & 15 \\ 15 & 18 & 10 \\ 12 & 12 & 1 \end{bmatrix} (\text{mod}\, 37) = \\ = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Deste modo, o deciframento é feito do seguinte modo:

$$t_1 = T^{-1}.c_1\,(\text{mod}\, 37) \Rightarrow \\ t_1 = \begin{bmatrix} 19 & 27 & 15 \\ 15 & 18 & 10 \\ 12 & 12 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 26 \\ 6 \end{bmatrix} (\text{mod}\, 37) \\ = \begin{bmatrix} 792 \\ 528 \\ 318 \end{bmatrix} (\text{mod}\, 37) \\ = \begin{bmatrix} 15 \\ 10 \\ 22 \end{bmatrix}.$$

De modo análogo, encontramos t_2, t_3 e t_4 que correspondem ao texto original.

3.2.6 Ciframento de Vigenère

O Ciframento de Vigenère é polialfabético e assimétrico, ou seja, o algoritmo de ciframento é diferente do algoritmo de deciframento. Nesse ciframento, escolheremos uma chave que é um vetor $k = (k_0, k_1, ..., k_{n-1})$ em $\mathbb{Z}_{37}^n$, isto é, um vetor com n coordenadas inteiras variando de 0 a 37. As letras do texto são numeradas : $t_0, t_1, t_2, ...t_l$.
Para cifrar o texto, a primeira letra é deslocada de k_0 posições e, assim por diante. Ou seja, o Ciframento de Vigenère é feito substituindo cada letra do texto $t_0t_1t_2, ...t_l$, por uma letra c_i, onde

$$c_i = 10 + (t_i + k_{i(\text{mod}\, n)})\,(\text{mod}\, S) \qquad (3)$$

onde S é o número de símbolos correspondente a uma tabela de codificação. Nesse caso tomemos a TABELA 1, como referência, assim $S = 37$.

Exemplo 14:
Texto: $FAMAT\_2008$.
Substituindo cada letra do texto por uma sequência de números, de acordo com a TABELA 1 temos:

F	A	M	A	T	_	2	0	0	8
t_0	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9
15	10	22	10	29	36	39	37	37	45

.

Escolhendo uma chave para o ciframento, seja ela: $k = (10, 15, 20, 7, 18)$
Começaremos cifrando $t_0 \equiv F$.
Como $t_0 = 15$, aplicando (3), temos:

$$\begin{aligned} c_0 &= 10 + (t_0 + k_{0(\mathrm{mod}\,5)}) \,(\mathrm{mod}\,37) \\ c_0 &= 10 + (15 + 10) \,(\mathrm{mod}\,37) \\ c_0 &= 10 + 25 \,(\mathrm{mod}\,37) \\ c_0 &= 35. \end{aligned}$$

Logo, $F \equiv Z$, de acordo com a TABELA 1.
Fazendo analogamente para o restante do texto, então o ciframento ficará: $FAMAT\_2008 \equiv ZZFRKJRUH\_$
Note que nessa criptografia, podemos ter duas letras diferentes do texto levando em duas letras iguais no ciframento. No caso acima, o F e o primeiro A do texto são ambos cifrados como Z. Do mesmo modo duas letras iguais do texto podem ser levadas em letras diferentes no ciframento, é o caso do A, que se repete duas vezes no texto, e quando cifrados correspondem a letras diferentes. O primeiro A do texto corresponde à letra Z e o segundo à letra R.
O Ciframento de Vigenère não é muito eficiente, pois para que o sistema seja seguro, é preciso que a mensagem seja grande e a chave aleatória que a cifra também. Isto significa que nos dias atuais os computadores teriam que trocar milhões de dígitos de chaves por dia, o que requer um gasto muito grande de tempo.

3.2.7 Sistemas de Rotores

Os sistemas de rotores são equipamentos elétricos compostos por discos (rotores) que tem por finalidade realizar uma substituição mais sofisticada. Essa criptografia é polialfabética e simétrica, ou seja, o algoritmo de ciframento e deciframento é o mesmo. Cada rotor é construído de modo que corresponda, matematicamente, a uma substituição monoalfabética. Nesses rotores são distribuidas, sob a forma de furos, todas as letras, algarismos e símbolos de um determinado alfabeto, de modo que esses furos estejam distribuidos como vértices de polígonos regulares inscritos nos rotores. Esses rotores podem ser girados de k posições, ou seja, girados de um ângulo de $k\frac{2\pi}{n}$ radianos, sendo n a quantidade total de símbolos do alfabeto.

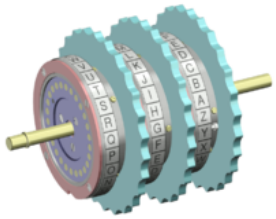

Figura 1: Três rotores.
(http://pt.wikipedia.org/wiki/Máquina_Enigma)

Figura 2: Interior da máquina Enigma, utilizada durante a II Guerra Mundial e que utiliza o Sistema de Rotores.
(http://users.telenet.be/d.rijmenants/pics/EnigmaInside.jpg)

Para facilitar a construção do equipamento, a mensagem a ser cifrada é dividida em blocos de 1000 símbolos. Em cada bloco, denotaremos por t_i o símbolo que está na i-ésima

posição, $i = 0, ..., 999$. Além disso, indicaremos por i_1, i_2 e i_3 as unidades, dezenas e centenas de i. Por exemplo, t_{23} corresponde a $i = 23$, $i_1 = 3$, $i_2 = 2$ e $i_3 = 0$.
Quando o sistema é girado de k posições em um determinado sentido (horário ou anti-horário), temos uma substituição monoalfabética que pode ser descrita como:

$$S' = -k + S(t_i + k),$$

sendo S uma substituição monoalfabética e t_i é um símbolo a ser cifrado, ou ainda

$$S'' = k + S(t_i - k)$$

se o giro for em sentido contrário.
Deste modo, todos os cálculos são feitos com mod n.
Para exemplificar, suponhamos que temos três rotores nos quais:
(i) S_1, S_2 e S_3 sejam as substituições monoalfabéticas com os três rotores em suas posições iniciais;
(ii) $t = t_0t_1t_2 \cdots t_{r-1}$ o texto a ser cifrado.
(iii) $c = c_0c_1c_2 \cdots c_{r-1}$ o texto cifrado;
Consideremos ainda uma substituição monoalfabética inicial que chamaremos de IP e uma substituição monoalfabética R de ordem 2, ou seja, uma transposição ($R = R^{-1}$). Assim, o ciframento pode ser feito pela seguinte operação:

$$\begin{aligned} c_i = IP^{-1}C_{-i_1}S_1^{-1}C_{i_1-i_2}S_2^{-1}C_{i_2-i_3}S_3^{-1}C_{i_3} \\ RC_{-i_3}S_3C_{i_3-i_2}S_2C_{i_2-i_1}S_1C_{i_1}IP(t_i), \end{aligned} \quad (4)$$

sendo C_m é uma *Substituição de César* de ordem m.
A chave do segredo do sistema de rotores compõem-se:
· Pela substituição IP;
· Pelas substituições S_1, S_2, S_3 e R;
· Pelas posições iniciais dos rotores;
Observação: Pela construção, R é uma involução, ou seja, R^2 é a identidade. Deste modo, no esquema acima, cifrar e decifrar é uma só operação.

Exemplo 15:
Sejam as substituições monoalfabéticas S_1, S_2 e S_3, descritas na Tabela 2.
Suponhamos que a palavra $FAMAT\_2008$ se encontre na posição

$$\cdots t_{352}, t_{353}, t_{354}, t_{355}, t_{356},$$
$$t_{357}, t_{358}, t_{359}, t_{360}, t_{361} \cdots$$

e queremos criptografá-la usando os rotores. Assim, para cifrar a primeira letra teremos os seguintes passos:
$F = t_{352}$, então temos que $i_1 = 2$, $i_2 = 5$ e $i_3 = 3$. Aplicando a fórmula (4), teremos os respectivos passos para cifrar:
1) $IP(t_{352}) = IP(F) = H$
2) $C_{i_1}(H) = C_2(H) = J$
3) $S_1(J) = B$
4) $C_{i_2-i_1}(B) = C_{5-2}(B) = C_3(B) = E$
5) $S_2(E) = K$
6) $C_{i_3-i_2}(K) = C_{3-5}(K) = C_{-2}(K) = I$
7) $S_3(I) = C$
8)$C_{-i_3}(C) = C_{-3}(C) = 9$
9) $R(9) = K$
10) $C_{i_3}(K) = C_3(K) = N$
11) $S_3^{-1}(N) = J$
12) $C_{i_2-i_3}(J) = C_{5-3}(J) = C_2(J) = L$
13) $S_2^{-1}(L) = N$
14) $C_{i_1-i_2}(N) = C_{2-5}(N) = C_{-3}(N) = K$
15) $S_1^{-1}(K) = A$
16) $C_{-i_1} = C_{-2}(A) = 8$
17) $(IP)^{-1}(8) = J$
Logo, o ciframento da letra F é o J. Para decifrar basta aplicar a mesma função (4). Vejamos o exemplo:
1) $IP(c_{352}) = IP(J) = 8$
2) $C_{i_1}(8) = A$
3) $S_1(A) = K$
4) $C_{i_2-i_1}(K) = C_{5-2}(K) = C_3(K) = N$
5) $S_2(N) = L$
6) $C_{i_3-i_2}(L) = C_{3-5}(L) = C_{-2}(L) = J$
7) $S_3(J) = N$
8)$C_{-i_3}(N) = C_{-3}(N) = K$
9) $R(K) = 9$
10) $C_{i_3}(9) = C_3(9) = C$
11) $S_3^{-1}(C) = I$
12) $C_{i_2-i_3}(I) = C_{5-3}(I) = C_2(I) = K$

13) $S_2^{-1}(K) = E$
14) $C_{i_1-i_2}(E) = C_{2-5}(E) = C_{-3}(E) = B$
15) $S_1^{-1}(B) = J$
16) $C_{-i_1} = C_{-2}(J) = H$
17) $(IP)^{-1}(H) = F$

S	S_1	S_2	S_3	IP	R
$10 \longleftrightarrow A$	K	Q	P	S	2
$11 \longleftrightarrow B$	F	W	0	K	N
$12 \longleftrightarrow C$	L	F	Y	2	Z
$13 \longleftrightarrow D$	Z	$-$	6	G	6
$14 \longleftrightarrow E$	1	K	A	0	0
$15 \longleftrightarrow F$	J	V	M	H	T
$16 \longleftrightarrow G$	I	3	9	V	1
$17 \longleftrightarrow H$	S	J	K	Q	8
$18 \longleftrightarrow I$	0	R	C	W	R
$19 \longleftrightarrow J$	B	U	N	8	S
$20 \longleftrightarrow K$	W	C	T	A	9
$21 \longleftrightarrow L$	P	Z	2	5	V
$22 \longleftrightarrow M$	7	2	Z	F	W
$23 \longleftrightarrow N$	H	L	8	R	B
$24 \longleftrightarrow O$	X	5	S	P	4
$25 \longleftrightarrow P$	T	D	H	Z	5
$26 \longleftrightarrow Q$	C	S	X	I	$-$
$27 \longleftrightarrow R$	4	8	B	C	I
$28 \longleftrightarrow S$	M	G	I	4	J
$29 \longleftrightarrow T$	G	N	O	J	F
$30 \longleftrightarrow U$	8	E	1	9	7
$31 \longleftrightarrow V$	$-$	4	D	U	L
$32 \longleftrightarrow W$	A	T	F	E	M
$33 \longleftrightarrow X$	N	1	U	6	X
$34 \longleftrightarrow Y$	2	H	3	L	3
$35 \longleftrightarrow Z$	V	7	5	X	C
$36 \longleftrightarrow -$	O	M	Q	T	Q
$37 \longleftrightarrow 0$	3	I	E	B	E
$38 \longleftrightarrow 1$	R	9	V	Y	G
$39 \longleftrightarrow 2$	6	Y	4	N	A
$40 \longleftrightarrow 3$	D	X	G	O	Y
$41 \longleftrightarrow 4$	Y	6	W	M	O
$42 \longleftrightarrow 5$	Q	A	J	$-$	P
$43 \longleftrightarrow 6$	5	0	$-$	7	D
$44 \longleftrightarrow 7$	E	O	R	D	U
$45 \longleftrightarrow 8$	9	B	7	1	H
$46 \longleftrightarrow 9$	U	P	L	3	K

Tabela 2

Logo ao aplicar a função (4), acontece o deciframento voltando ao texto original, como era esperado. De modo análogo fazemos isto para o restante da mensagem a ser criptografada e obtemos os seguintes resultados:
Cifrando o texto:

$$FAMAT\_2008 \rightarrow JAICIX7ESY.$$

E deciframento o texto:

$$JAICIX7ESY \rightarrow FAMAT\_2008.$$

3.2.8 O Método MH (Merkle e Hellman)

Esse método é monoalfabético e assimétrico pois o algoritmo de ciframento é diferente do algoritmo de deciframento.

A segurança do Método MH (Merkle e Hellman) se baseia na dificuldade do chamado *Problema da Mochila.*

O Problema da Mochila
Dado o vetor $a = (a_1, a_2, ..., a_n)$ de coordenadas naturais e b também natural, o problema da mochila consiste em saber se existe $X = (x_1, x_2, ..., x_n)$ onde cada x_i é 0 ou 1, tal que:

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

Exemplo 16:
Sejam $n = 6$, $b = 14$ e $a_1 = 2$, $a_2 = 3$, $a_3 = 5$, $a_4 = 7$, $a_5 = 8$ e $a_6 = 12$.
Logo, a solução deste problema será dado por $x_1 = 1$, $x_2 = 0$, $x_3 = 1$, $x_4 = 1$, $x_5 = 0$ e $x_6 = 0$, pois

$$\sum_{i=1}^{n} a_i x_i = b \Rightarrow$$
$$2.1 + 3.0 + 5.1 + 7.1 + 8.0 + 12.0 = 14.$$

Definimos a *chave pública* de cada destinatário no Método MH pelo vetor

$$P = (c_1, c_2, ..., c_n)$$

de naturais, onde $n \approx 100$.

Para cifrar uma mensagem e enviar ao destinatário, o emissor deve consultar a chave pública $P = (c_1, c_2, ..., c_n)$ do destinatário, conveter cada símbolo da mensagem original em números naturais m menores do que 2^n e escrevê-lo na base binária, isto é,

$$m = [m_1 m_2 ... m_n]_2 ,$$

sendo $m_i = 0$ ou 1. Então, calcula-se

$$P(m) = \sum_{i=1}^{n} m_i c_i .$$

Assim, o trabalho do destinatário em decifrar $P(m)$ é determinar a solução do problema da mochila sabendo-se

$$P = (c_1, c_2, ..., c_n) \text{ e } P(m).$$

Para que o problema da mochila seja de fácil resolução, a chave pública não pode ser qualquer. Deste modo, para decifrar a mensagem o destinatário deve inicialmente antes de divulgar a sua chave pública, criar uma seqüência de números naturais

$$s = (s_1, s_2, ..., s_n) \tag{5}$$

e também t e k tais que

$$\sum_{i=1}^{r} s_i < s_{r+1} < t$$

para $1 \leq r < n-1$ e $\text{mdc}(k, t) = 1$.
Assim, a seqüência $s = (s_1, s_2, ..., s_n)$ é essencial para a solução do problema da mochila. O destinatário mantém o vetor s e os valores de t e k secretos e publica o vetor c, dado por

$$c_i = k s_i \,(\text{mod}\, t) ,$$

com $1 \leq i \leq n$. Além disso, o emissor escolhe e mantém secreto o número l que deve satisfazer a equação:

$$lk \,(\text{mod}\, t) = 1.$$

Algoritmo para a Resolução do Problema da Mochila

Algoritmo da mochila
Entrada: $(n, (s_1, s_2, ..., s_n), d)$, onde

$$s = (s_1, s_2, ..., s_n)$$

é a seqüência (5) e

$$d \equiv l.P\,(m) \,(\text{mod}\, t) .$$

Saída: m.
Etapa 1: Faça $y = d$.
Etapa 2: Para cada $i = n$, $n-1$, $n-2$, ...1, ou seja, para os valores de i serão atribuidos uma seqüência decrescente de n até 1, faça:
(1) Se $y < s_i$, então, $m_i = 0$.
(2) Se $y \geq s_i$, então faça $y = y - s_i$ e tome $m_i = 1$.
Etapa 3:
(1) Se $y = 0$, então retorne o vetor:
$m = (m_1, m_2, ..., m_n)$.
(2) Se $y \neq 0$, então o problema da mochila não tem solução.

Exemplo 17:
Seja a mensagem $FAMAT\_2008$. Associando a mensagem ao números correspondentes na Tabela 1, temos a sequência de números:

15 10 22 10 29 36 39 37 37 45

Passando para a base binária a sequência de números acima, temos:

$$15 = [001111]_2$$
$$10 = [001010]_2$$
$$22 = [010110]_2$$
$$10 = [001010]_2$$
$$29 = [011101]_2$$
$$36 = [100100]_2$$
$$39 = [100111]_2$$
$$37 = [100101]_2$$
$$37 = [100101]_2$$
$$45 = [101101]_2$$

Precisamos agora de determinar a chave pública que será o vetor $P = (c_1, c_2, ..., c_n)$. Para o destinátario determinar a chave

pública, primeiro ele deverá escolher uma seqüência s como em (5). Além disso, k e t, de modo que $\sum_{i=1}^{n} s_i < t$ e $\text{mdc}\,(k,t) = 1$.
Para o exemplo escolhemos a sequência:

$$s = (5, 7, 14, 27, 55, 109)$$

e $k = 50$ e $t = 229$, pois $\text{mdc}\,(50, 229) = 1$ e $t > 5 + 7 + ... + 109 = 217$.
Temos então a expressão:

$$50l \,(\text{mod}\, 229) = 1 \Rightarrow 229x + 50l = 1.$$

Calculemos o valor de l a partir do *Algoritmo Euclidiano Estendido.*
Colocando os valores em uma tabela:

i	Restos	Quocientes	x_i	y_i
-1	229	$*$	1	0
0	50	$*$	0	1
1	29	4	1	-4
2	21	1	-1	5
3	8	1	2	-9
4	5	2	-5	23
5	3	1	7	-32
6	2	1	-12	55
7	1	1	19	-87

Temos

$$l = y_7 = -87.$$

Mas não nos interessa trabalhar com valores de l negativos, para isso temos o algoritmo derivado do teorema da solução geral de uma equação diofantina que encontra um valor positivo para l. (Veja o tópico "Algoritmo Para Reverter Valores de d Negativos" na seção "Criptografia RSA")

Etapa 1) Calcular o valor de l normalmente.
Etapa 2) Se $l < 0$, então faça:

$$\bar{l} = l + 229j$$

para j inteiro de tal modo que $\bar{l} > 0$.
Etapa 3) Faça $l = \bar{l}$.

Logo, para o exemplo anterior:

$$\bar{l} = -87 + 229j, \text{ para } j = 1$$
$$\bar{l} = 229 - 87$$
$$\bar{l} = 142$$
$$l = \bar{l} = 142.$$

Deste modo, após encontrar o novo valor de l (positivo), então continua-se o ciframento e o deciframento do Método de MH.
Deste modo o destinátario pública o vetor $c = (c_1, c_2, ..., c_n)$, onde $n = 6$ e cujo:

$$c_i = ks_i \,(\text{mod}\, t)\,.$$

Assim temos que a chave pública é

$$P = (21, 121, 13, 205, 2, 183).$$

Logo, a primeira letra da mensagem, que é F, que corresponde a $15 = [001111]_2$ é cifrada em

$$P(15) = \sum_{i=1}^{n} m_i c_i =$$
$$0.21 + 0.121 + 1.13 + 1.205 +$$
$$+1.2 + 1.183 = 403$$

Procedendo de modo análogo com os demais símbolos da mensagem, temos

$$403 \quad 2 \quad 328 \quad 2 \quad 522 \quad 226$$
$$411 \quad 409 \quad 409 \quad 422.$$

Para decifrar a mensagem o destinatário deve primeiro determinar os valores de

$$d = l.P(m) \,(\text{mod}\, t)\,.$$

Para o exemplo vamos ter:
Para $P(15)$ então $d = 205$.
Para $P(10)$ então $d = 55$.
Para $P(22)$ então $d = 89$.
Para $P(29)$ então $d = 157$.
Para $P(36)$ então $d = 32$.
Para $P(39)$ então $d = 196$.
Para $P(37)$ então $d = 141$.
Para $P(45)$ então $d = 155$.

Continuando o deciframento do Método MH, vamos começar decifrando a primeira letra da nossa mensagem utilizando para isso o *Algoritmo da Mochila.*

Temos: $(n, (s_1, s_2, ..., s_n), d)$,que corresponde a $(6, (5, 7, 14, 27, 55, 109), 205)$.
Etapa 1: Faça $y = 205$.
Etapa 2:
Para $i = 6$:
Como $y \geq s_6$, ou seja, $y \geq 109$ então faça $y = 205 - 109 = 96$ e tome $m_6 = 1$.
Para $i = 5$:
Como $y \geq s_5$, ou seja, $y \geq 55$ então faça $y = 96 - 55 = 41$ e tome $m_5 = 1$.
Para $i = 4$:
Como $y \geq s_4$, ou seja, $y \geq 27$ então faça $y = 41 - 27 = 14$ e tome $m_4 = 1$.
Para $i = 3$:
Como $y \geq s_3$, ou seja, $y \geq 14$ então faça $y = 14 - 14 = 0$ e tome $m_3 = 1$.
Para $i = 2$:
Como $y < s_2$, ou seja, $y < 7$ então tome $m_2 = 0$.
Para $i = 1$:
Como $y < s_1$, ou seja, $y < 5$ então tome $m_1 = 0$.
Etapa 3: Como $y = 0$, então

$$m = [001111]_2 = 15,$$

que corresponde à letra F.

De modo análogo, utilizando o Algoritmo da Mochila para os demais símbolos da mensagem, encontramos os respectivos resultados:

$$[000010]_2, [010110]_2, [000010]_2, [011101]_2, [100100]_2, [100111]_2, [100101]_2, [100101]_2, [101101]_2$$

que correspondem a

$$m = 10, m = 22, m = 10, m = 29, m = 36, m = 39, m = 37, m = 37, m = 45.$$

Formando a mensagem inicial $FAMAT\_2008$.

3.2.9 Data Encryption Standard (DES)

O DES consiste de um algoritmo de criptografia simétrico e polialfabético com entrada e saída binárias. Sendo assim, uma mensagem a ser enviada deve ser convertida em uma seqüência binária.
Assim como em qualquer esquema de criptografia, o algoritmo precisa de duas entradas: a mensagem a ser enviada e, portanto, codificada e a chave, que é a "senha" que irá manter a transmissão sigilosa.
A mensagem original convertida em uma seqüência binária é dividida em blocos M que podem ser de 64 dígitos cada.
Consideremos a função I que permuta a posição dos 64 dígitos do bloco M. Geralmente I é definida por uma tabela.
Para efeito de compreensão do algoritmo, chamemos a imagem $I(M)$ de N_0 de descrevamos uma rodada do algoritmo (geralmente são realizadas 16 rodadas):

(i) Dividamos o bloco N_0 de 64 dígitos em duas partes: a parte "esquerda", que chamaremos de E_0 e a parte "direita" que chamaremos de D_0.
(ii) Consideremos a função X que expande o bloco D_0, de 32 dígitos, para um bloco $X(D_0)$ de 48 dígitos. Além da expansão, nessa etapa temos também uma permutação de dígitos, uma vez que, à semelhança de I, X é dada por uma tabela.
(iii) Consideremos um bloco aleatório de 48 dígito binário que denotaremos por K_1. Esse bloco é parte das chaves do sistema criptográfico (para cada rodada há uma chave).
(iv) Uma soma binária dígito a dígito entre $X(D_0)$ e K_1 é realizada.
(v) O bloco $X(D_0) + K_1$ é dividido em blocos $B_1, ..., B_8$ de 6 dígitos cada e, utilizando 8 funções redutoras $S_1, ..., S_8$. Essas funções transformam B_i de 6 dígitos em blocos B_i' de 4 dígitos. De um modo geral, essas funções redutoras são dadas por tabelas e a manipulação dessas tabelas será exemplificada

abaixo. Deste modo, o bloco $X(D_0) + K_1$ é transformado em um bloco S de 32 dígitos.
(*vi*) Uma outra permutação de dígitos P é aplicada ao bloco S.
(*vii*) Uma outra soma binária dígito a dígito é feita entre o bloco $P(S)$ e o bloco E_0. Essa soma é chamada de D_1.
(*viii*) Definimos o bloco E_1 como sendo o bloco D_0.
(*ix*) Um novo bloco N_1 é formado pela junção do bloco E_1 com o bloco D_1 formado acima.

O bloco N_1 é submetido a uma nova rodada conforme descrito acima e obtemos N_2, N_3 até N_{16}.
Após as 16 rodadas, é realizada uma troca de lados em N_{16} entre os blocos E_{16} e D_{16}. Chamemos essa troca de T. Assim, $T(E_{16}) = D'_{16}$ e $T(D_{16}) = E'_{16}$ e, temos um novo bloco $T(N_{16}) = N'_{16}$.
Por fim, a inversa da função permutação I, ou seja, I^{-1} é aplicada em N'_{16} e este é o bloco cifrado, que chamaremos de C. Assim, $I^{-1}(N'_{16}) = C$.

Simplificando, temos a seguinte composta:

$$I(M) = N_0 = E_0 D_0 \Rightarrow$$
$$X \circ I(M) = E_0 X(D_0) \Rightarrow$$
$$K_1 \circ X \circ I(M) = E_0 [X(D_0) + K_1] =$$
$$= E_0 [B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8] \Rightarrow$$
$$S \circ K_1 \circ X \circ I(M) =$$
$$= E_0 [S_1(B_1) S_2(B_2) ... S_7(B_7) S_8(B_8)]$$
$$S \circ K_1 \circ X \circ I(M) = E_0 [B'_1 B'_2 B'_3 B'_4 B'_5 B'_6 B'_7 B'_8] \Rightarrow$$
$$S \circ K_1 \circ X \circ I(M) = E_0 S \Rightarrow$$
$$P \circ S \circ K_1 \circ X \circ I(M) = E_0 P(S) \Rightarrow$$
$$E_0 \circ P \circ S \circ K_1 \circ X \circ I(M) = [E_0 + P(S)] \Rightarrow$$
$$D_0 \circ E_0 \circ P \circ S \circ K_1 \circ X \circ I(M) = D_0 [E_0 + P(S)] \Rightarrow$$
$$D_0 \circ E_0 \circ P \circ S \circ K_1 \circ X \circ I(M) = D_0 D_1 \Rightarrow$$
$$D_0 \circ E_0 \circ P \circ S \circ K_1 \circ X \circ I(M) = E_1 D_1 \Rightarrow$$
$$D_0 \circ E_0 \circ P \circ S \circ K_1 \circ X \circ I(M) = N_1.$$

Chamando $D_0 \circ E_0 \circ P \circ S \circ K_1 \circ X = Z_1$. Logo,

$$Z_1 \circ I(M) = N_1.$$

Aplicando 16 rodadas, temos:

$$Z_{16} \circ ... \circ Z_1 \circ I(M) = N_{16} \Rightarrow$$
$$T \circ Z_{16} \circ ... \circ Z_1 \circ I(M) = N'_{16} \Rightarrow$$
$$I^{-1} \circ T \circ Z_{16} \circ ... \circ Z_1 \circ I(M) = C.$$

Chamando $I^{-1} \circ T \circ Z_{16} \circ ... \circ Z_1 \circ I = DES$, temos

$$DES(M) = C.$$

Como o algoritmo é simétrico, para decifrar C, basta aplicá-lo novamente, ou seja:

$$DES(C) = M.$$

Exemplo 18:
Consideremos as seguintes tabelas para construção da Criptografia DES:

59_1	51_2	43_3	35_4	27_5	19_6	11_7	03_8
57_9	49_{10}	41_{11}	33_{12}	25_{13}	17_{14}	09_{15}	01_{16}
60_{17}	52_{18}	44_{19}	36_{20}	28_{21}	20_{22}	12_{23}	04_{24}
58_{25}	50_{26}	42_{27}	34_{28}	26_{29}	18_{30}	10_{31}	02_{32}
64_{33}	56_{34}	48_{35}	40_{36}	32_{37}	24_{38}	16_{39}	08_{40}
62_{41}	54_{42}	46_{43}	38_{44}	30_{45}	22_{46}	14_{47}	06_{48}
63_{49}	55_{50}	47_{51}	39_{52}	31_{53}	23_{54}	15_{55}	07_{56}
61_{57}	53_{58}	45_{59}	37_{60}	29_{61}	21_{62}	13_{63}	05_{64}

TABELA 3: Função permutação I

16_1	32_2	8_3	24_4	64_5	48_6	56_7	40_8
15_9	31_{10}	7_{11}	23_{12}	63_{13}	47_{14}	55_{15}	39_{16}
14_{17}	30_{18}	6_{19}	22_{20}	62_{21}	46_{22}	54_{23}	38_{24}
13_{25}	29_{26}	5_{27}	21_{28}	61_{29}	45_{30}	53_{31}	37_{32}
12_{33}	28_{34}	4_{35}	20_{36}	60_{37}	44_{38}	52_{39}	36_{40}
11_{41}	27_{42}	3_{43}	19_{44}	59_{45}	43_{46}	51_{47}	35_{48}
10_{49}	26_{50}	2_{51}	18_{52}	58_{53}	42_{54}	50_{55}	34_{56}
9_{57}	25_{58}	1_{59}	17_{60}	57_{61}	41_{62}	49_{93}	33_{64}

TABELA 4: Função permutação I^{-1}

15_1	16_2	17_3	18_4	32_5	1_6
19_7	20_8	21_9	22_{10}	2_{11}	3_{12}
23_{13}	24_{14}	25_{15}	26_{16}	4_{17}	5_{18}
27_{19}	28_{20}	29_{21}	30_{22}	6_{23}	7_{24}
31_{25}	32_{26}	1_{27}	2_{28}	8_{29}	9_{30}
3_{31}	4_{32}	5_{33}	6_{34}	10_{35}	11_{36}
7_{37}	8_{38}	9_{39}	10_{40}	12_{41}	13_{42}
11_{43}	12_{44}	13_{45}	14_{46}	14_{47}	15_{48}

TABELA 5: função expansão X

25_1	26_2	27_3	15_4	16_5	17_6	28_7	29_8
1_9	18_{10}	19_{11}	2_{12}	20_{13}	21_{14}	3_{15}	4_{16}
13_{17}	14_{18}	30_{19}	31_{20}	32_{21}	8_{22}	9_{23}	10_{24}
22_{25}	23_{26}	24_{27}	11_{28}	12_{29}	5_{30}	6_{31}	7_{32}

TABELA 6: Função permutação P

As tabelas das páginas 26 e 27 são rotuladas de TABELAS 7: Caixas S.

Seja a mensagem $FAMAT\_2008$. Suponhamos que o emissor A, queira enviar essa

mensagem ao receptor B usando a Criptografia DES. Assim, A associa a mensagem aos números correspondentes na TABELA 1, obtendo a seqüencia de números:

$$15\ 10\ 22\ 10\ 29\ 36\ 39\ 37\ 37\ 45,$$

que, respectivamente, na base binária são:

$$001111\ 000010\ 010110\ 000010\ 011101$$
$$100100\ 100111\ 100101\ 100101\ 101101.$$

Agrupando a seqüencia de bits em blocos de 64 bits temos:

$$M = 0011110000100101100000100111011 \quad (6)$$
$$0010010011110010110010110110100 00.$$

Note que tinhamos apenas 60 bits. Os bits que ficaram faltando para completar um bloco de 64 bits foram obtidos acrescentando-se 4 zeros ao final da seqüência.

Logo, para o início do processo, a mensagem passa pela primeira fase que é a função permutação I, a partir da TABELA 3, no qual é obtida pela seqüência a seguir:

$$I(M) = N_0 = 0010101111100110 \quad (7)$$
$$1100100110111000001100 10$$
$$0110101101001100000101 01.$$

O n-ésimo bit de (7) é o m-ésimo bit de (6), sendo que m e n estão relacionados de acordo com a entrada m_n da TABELA 3. Por exemplo, se $n = 1$, a TABELA 3 fornece $m = 59$. Logo, o 1º. bit de (7) é o 59º. bit de (6) e assim, por diante.

Separando (7) em blocos de 32 bits, obtemos dois blocos. Chamaremos os primeiros 32 bits de bloco da "esquerda" e denotaremos por "E_0" e os outros 32 bits restantes de bloco da "direita" e denotaremos por "D_0". Assim,

$$E_0 = 00101011111001101100100110111000$$
$$D_0 = 00110010011010110100110000010101 \quad (8)$$

Para o bloco D_0 faremos uma expansão usando a TABELA 5, dada anteriormente. Assim, essa seqüência de 32 bits será transformada em uma nova seqüência com 48 bits, dada por:

$$X(D_0) = 110110001101000010010 \quad (9)$$
$$101000011001110010110 1001.$$

O n-ésimo bit de (9) é o m-ésimo bit de (8), sendo que m e n estão relacionados de acordo com a entrada m_n da TABELA 5.

Por exemplo, se $n = 1$, a TABELA 5 fornece $m = 15$. Logo, o 1º. bit de (9) é o 15º. bit de (8) e assim, por diante.
Consideremos uma seqüência binária de 48 bits, que será a chave (que deve ser mantida em sigilo pelos comunicantes):

$$K_1 = 111101101010010010100 01$$
$$100011001011010011101 0001.$$

Fazendo a soma binária, dígito a dígito, dos 48 bits do bloco $X(D_0)$ com a chave K_1, temos a nova seqüência:

$$X(D_0) + K_1 = 001011100111010000110 11$$
$$001011010010100001011 1000.$$

Usaremos agora, as Caixas S para comprimir a seqüência acima de 48 bits para 32 bits binários. Primeiramente, dividiremos a seqüência anterior em blocos de 6 bits obtendo: B_1 o primeiro bloco, B_2 o segundo bloco até o oitavo bloco:

$$\underbrace{001011}_{B_1}\ \underbrace{100111}_{B_2}\ \underbrace{010000}_{B_3}\ \underbrace{110110}_{B_4}$$
$$\underbrace{010110}_{B_5}\ \underbrace{100101}_{B_6}\ \underbrace{000010}_{B_7}\ \underbrace{111000}_{B_8}.$$

S_1

$1_{0,0}$	$12_{0,1}$	$9_{0,2}$	$5_{0,3}$	$10_{0,4}$	$15_{0,5}$	$6_{0,6}$	$2_{0,7}$	$8_{0,8}$	$11_{0,9}$	$4_{0,10}$	$14_{0,11}$	$7_{0,12}$	$12_{0,13}$	$13_{0,14}$	$2_{0,15}$
$7_{1,0}$	$10_{1,1}$	$2_{1,2}$	$6_{1,3}$	$14_{1,4}$	$3_{1,5}$	$11_{1,6}$	$9_{1,7}$	$15_{1,8}$	$0_{1,9}$	$4_{1,10}$	$12_{1,11}$	$1_{1,12}$	$5_{1,13}$	$3_{1,14}$	$13_{1,15}$
$9_{2,0}$	$0_{2,1}$	$15_{2,2}$	$1_{2,3}$	$2_{2,4}$	$10_{2,5}$	$3_{2,6}$	$11_{2,7}$	$4_{2,8}$	$5_{2,9}$	$13_{2,10}$	$6_{2,11}$	$12_{2,12}$	$7_{2,13}$	$14_{2,14}$	$8_{2,15}$
$0_{3,0}$	$9_{3,1}$	$2_{3,2}$	$12_{3,3}$	$10_{3,4}$	$8_{3,5}$	$15_{3,6}$	$3_{3,7}$	$7_{3,8}$	$11_{3,9}$	$6_{3,10}$	$1_{3,11}$	$4_{3,12}$	$13_{3,13}$	$5_{3,14}$	$14_{3,15}$

S_2

$1_{0,0}$	$10_{0,1}$	$11_{0,2}$	$7_{0,3}$	$2_{0,4}$	$14_{0,5}$	$8_{0,6}$	$15_{0,7}$	$6_{0,8}$	$9_{0,9}$	$12_{0,10}$	$0_{0,11}$	$5_{0,12}$	$3_{0,13}$	$13_{0,14}$	$4_{0,15}$
$7_{1,0}$	$10_{1,1}$	$0_{1,2}$	$5_{1,3}$	$6_{1,4}$	$1_{1,5}$	$11_{1,6}$	$2_{1,7}$	$13_{1,8}$	$12_{1,9}$	$3_{1,10}$	$8_{1,11}$	$14_{1,12}$	$9_{1,13}$	$4_{1,14}$	$15_{1,15}$
$14_{2,0}$	$5_{2,1}$	$7_{2,2}$	$11_{2,3}$	$13_{2,4}$	$0_{2,5}$	$2_{2,6}$	$8_{2,7}$	$10_{2,8}$	$1_{2,9}$	$4_{2,10}$	$15_{2,11}$	$3_{2,12}$	$6_{2,13}$	$9_{2,14}$	$12_{2,15}$
$8_{3,0}$	$2_{3,1}$	$14_{3,2}$	$9_{3,3}$	$15_{3,4}$	$5_{3,5}$	$6_{3,6}$	$11_{3,7}$	$7_{3,8}$	$12_{3,9}$	$1_{3,10}$	$0_{3,11}$	$4_{3,12}$	$14_{3,13}$	$10_{3,14}$	$3_{3,15}$

S_3

$0_{0,0}$	$9_{0,1}$	$4_{0,2}$	$2_{0,3}$	$11_{0,4}$	$7_{0,5}$	$1_{0,6}$	$12_{0,7}$	$13_{0,8}$	$6_{0,9}$	$14_{0,10}$	$8_{0,11}$	$5_{0,12}$	$3_{0,13}$	$10_{0,14}$	$15_{0,15}$
$4_{1,0}$	$2_{1,1}$	$9_{1,2}$	$3_{1,3}$	$5_{1,4}$	$13_{1,5}$	$14_{1,6}$	$6_{1,7}$	$15_{1,8}$	$11_{1,9}$	$1_{1,10}$	$7_{1,11}$	$10_{1,12}$	$12_{1,13}$	$8_{1,14}$	$0_{1,15}$
$1_{2,0}$	$12_{2,1}$	$7_{2,2}$	$10_{2,3}$	$4_{2,4}$	$15_{2,5}$	$9_{2,6}$	$6_{2,7}$	$3_{2,8}$	$8_{2,9}$	$13_{2,10}$	$11_{2,11}$	$0_{2,12}$	$14_{2,13}$	$2_{2,14}$	$5_{2,15}$
$14_{3,0}$	$5_{3,1}$	$10_{3,2}$	$2_{3,3}$	$8_{3,4}$	$9_{3,5}$	$0_{3,6}$	$11_{3,7}$	$12_{3,8}$	$3_{3,9}$	$1_{3,10}$	$6_{3,11}$	$15_{3,12}$	$7_{3,13}$	$4_{3,14}$	$13_{3,15}$

S_4

$9_{0,0}$	$14_{0,1}$	$0_{0,2}$	$13_{0,3}$	$15_{0,4}$	$3_{0,5}$	$5_{0,6}$	$8_{0,7}$	$6_{0,8}$	$11_{0,9}$	$10_{0,10}$	$7_{0,11}$	$1_{0,12}$	$4_{0,13}$	$12_{0,14}$	$2_{0,15}$
$6_{1,0}$	$8_{1,1}$	$9_{1,2}$	$3_{1,3}$	$10_{1,4}$	$15_{1,5}$	$0_{1,6}$	$5_{1,7}$	$1_{1,8}$	$13_{1,9}$	$7_{1,10}$	$4_{1,11}$	$12_{1,12}$	$2_{1,13}$	$11_{1,14}$	$14_{1,15}$
$14_{2,0}$	$0_{2,1}$	$3_{2,2}$	$6_{2,3}$	$5_{2,4}$	$12_{2,5}$	$9_{2,6}$	$15_{2,7}$	$8_{2,8}$	$7_{2,9}$	$13_{2,10}$	$10_{2,11}$	$11_{2,12}$	$1_{2,13}$	$2_{2,14}$	$4_{2,15}$
$13_{3,0}$	$3_{3,1}$	$15_{3,2}$	$0_{3,3}$	$1_{3,4}$	$9_{3,5}$	$14_{3,6}$	$8_{3,7}$	$10_{3,8}$	$4_{3,9}$	$5_{3,10}$	$6_{3,11}$	$7_{3,12}$	$12_{3,13}$	$2_{3,14}$	$11_{3,15}$

S_5

$6_{0,0}$	$8_{0,1}$	$2_{0,2}$	$12_{0,3}$	$3_{0,4}$	$7_{0,5}$	$0_{0,6}$	$15_{0,7}$	$9_{0,8}$	$1_{0,9}$	$11_{0,10}$	$4_{0,11}$	$14_{0,12}$	$5_{0,13}$	$13_{0,14}$	$10_{0,15}$
$14_{1,0}$	$12_{1,1}$	$0_{1,2}$	$2_{1,3}$	$6_{1,4}$	$11_{1,5}$	$4_{1,6}$	$8_{1,7}$	$10_{1,8}$	$9_{1,9}$	$5_{1,10}$	$15_{1,11}$	$7_{1,12}$	$3_{1,13}$	$1_{1,14}$	$13_{1,15}$
$0_{2,0}$	$4_{2,1}$	$10_{2,2}$	$5_{2,3}$	$13_{2,4}$	$6_{2,5}$	$15_{2,6}$	$2_{2,7}$	$7_{2,8}$	$12_{2,9}$	$3_{2,10}$	$14_{2,11}$	$8_{2,12}$	$11_{2,13}$	$9_{2,14}$	$15_{2,15}$
$15_{3,0}$	$11_{3,1}$	$4_{3,2}$	$8_{3,3}$	$13_{3,4}$	$6_{3,5}$	$0_{3,6}$	$12_{3,7}$	$5_{3,8}$	$14_{3,9}$	$2_{3,10}$	$9_{3,11}$	$1_{3,12}$	$3_{3,13}$	$10_{3,14}$	$7_{3,15}$

S_6

$7_{0,0}$	$12_{0,1}$	$0_{0,2}$	$5_{0,3}$	$14_{0,4}$	$3_{0,5}$	$9_{0,6}$	$10_{0,7}$	$1_{0,8}$	$11_{0,9}$	$15_{0,10}$	$6_{0,11}$	$4_{0,12}$	$8_{0,13}$	$2_{0,14}$	$13_{0,15}$
$2_{1,0}$	$9_{1,1}$	$14_{1,2}$	$0_{1,3}$	$11_{1,4}$	$6_{1,5}$	$5_{1,6}$	$12_{1,7}$	$4_{1,8}$	$7_{1,9}$	$3_{1,10}$	$10_{1,11}$	$8_{1,12}$	$13_{1,13}$	$15_{1,14}$	$1_{1,15}$
$8_{2,0}$	$5_{2,1}$	$3_{2,2}$	$15_{2,3}$	$13_{2,4}$	$10_{2,5}$	$6_{2,6}$	$0_{2,7}$	$2_{2,8}$	$14_{2,9}$	$12_{2,10}$	$9_{2,11}$	$1_{2,12}$	$4_{2,13}$	$11_{2,14}$	$7_{2,15}$
$11_{3,0}$	$6_{3,1}$	$5_{3,2}$	$3_{3,3}$	$0_{3,4}$	$9_{3,5}$	$12_{3,6}$	$15_{3,7}$	$13_{3,8}$	$8_{3,9}$	$10_{3,10}$	$4_{3,11}$	$14_{3,12}$	$7_{3,13}$	$1_{3,14}$	$2_{3,15}$

S_7

$10_{0,0}$	$6_{0,1}$	$9_{0,2}$	$13_{0,3}$	$5_{0,4}$	$4_{0,5}$	$14_{0,6}$	$0_{0,7}$	$8_{0,8}$	$1_{0,9}$	$11_{0,10}$	$7_{0,11}$	$15_{0,12}$	$12_{0,13}$	$2_{0,14}$	$3_{0,15}$
$2_{1,0}$	$12_{1,1}$	$0_{1,2}$	$3_{1,3}$	$10_{1,4}$	$14_{1,5}$	$4_{1,6}$	$13_{1,7}$	$9_{1,8}$	$11_{1,9}$	$6_{1,10}$	$15_{1,11}$	$1_{1,12}$	$5_{1,13}$	$7_{1,14}$	$8_{1,15}$
$0_{2,0}$	$7_{2,1}$	$13_{2,2}$	$8_{2,3}$	$6_{2,4}$	$1_{2,5}$	$9_{2,6}$	$3_{2,7}$	$10_{2,8}$	$2_{2,9}$	$14_{2,10}$	$4_{2,11}$	$5_{2,12}$	$15_{2,13}$	$11_{2,14}$	$12_{2,15}$
$15_{3,0}$	$3_{3,1}$	$10_{3,2}$	$2_{3,3}$	$8_{3,4}$	$9_{3,5}$	$4_{3,6}$	$14_{3,7}$	$5_{3,8}$	$12_{3,9}$	$7_{3,10}$	$1_{3,11}$	$11_{3,12}$	$0_{3,13}$	$13_{3,14}$	$6_{3,15}$

S_8

$15_{0,0}$	$12_{0,1}$	$8_{0,2}$	$2_{0,3}$	$4_{0,4}$	$9_{0,5}$	$1_{0,6}$	$7_{0,7}$	$5_{0,8}$	$11_{0,9}$	$3_{0,10}$	$14_{0,11}$	$10_{0,12}$	$0_{0,13}$	$6_{0,14}$	$13_{0,15}$
$10_{1,0}$	$6_{1,1}$	$9_{1,2}$	$0_{1,3}$	$12_{1,4}$	$11_{1,5}$	$7_{1,6}$	$13_{1,7}$	$15_{1,8}$	$1_{1,9}$	$3_{1,10}$	$14_{1,11}$	$5_{1,12}$	$2_{1,13}$	$8_{1,14}$	$4_{1,15}$
$1_{2,0}$	$4_{2,1}$	$11_{2,2}$	$13_{2,3}$	$12_{2,4}$	$3_{2,5}$	$7_{2,6}$	$14_{2,7}$	$10_{2,8}$	$15_{2,9}$	$6_{2,10}$	$8_{2,11}$	$0_{2,12}$	$5_{2,13}$	$9_{2,14}$	$2_{2,15}$
$13_{3,0}$	$2_{3,1}$	$8_{3,2}$	$4_{3,3}$	$6_{3,4}$	$15_{3,5}$	$11_{3,6}$	$1_{3,7}$	$10_{3,8}$	$9_{3,9}$	$3_{3,10}$	$14_{3,11}$	$5_{3,12}$	$0_{3,13}$	$12_{3,14}$	$7_{3,15}$

Os blocos B_i serão reduzidos a quatro bits cada utilizando-se as Caixas S_i do seguinte modo:
O primeiro e último dígitos de B_i formam, em decimal, um número x de 0 a 3, que corresponde a uma das quatro linhas de S_i. Os quatro dígitos intermediários de B_i formam, em decimal, um número y de 0 a 15, que corresponde a uma das 16 colunos de S_i. Assim, localizamos o número $s_{x,y}$ na tabela S_i. O número s é um número de 0 a 15, que em binário, corresponde a uma seqüência B_i' de quatro dígitos que será colocada no lugar de B_i.
Por exemplo, no primeiro bloco

$$B_1 = 001011,$$

temos que o primeiro e o último dígitos, 0 e 1, formam o número binário 01, que em decimal é o número 1, ou seja, temos a segunda linha de S_1. Os quatro dígitos do meio de B_1 formam o número binário 0101, que em decimal é o número 5, que corresponde à sexta coluna de S_1. Logo, localizamos $s_{x,y} = 3_{1,5}$, ou seja, $s = 3$, que em binário é 0011. Assim $B_1 = 001011$ é substituído por $B_1' = 0011$.
De modo analógo para o restante dos blocos vamos obter: $B_2' = 1001$, $B_3' = 1101$, $B_4' = 1010$, $B_5' = 0100$, $B_6' = 0101$, $B_7' = 0110$, $B_8' = 0000$. Juntando todos os blocos B_i', para $i = 1, 2, ...8$, em uma só seqüência obtemos:

$$S = 00111001110110100100010101100000.$$

Usando a Tabela 6, fazemos uma nova permutação da seqüência acima à semelhança da que fizemos na seqüência (6) a qual chamaremos de $P(S)$:

$$P(S) = 011100000100001 \\ 11000011110101100.$$

Fazendo a soma binária de $E_0 + P(S)$ temos:

$$D_1 = E_0 + P(S) = 0101101110 \\ 100101010011100010100.$$

Juntando, respectivamente, as seqüências D_0 e D_1 temos:

$$N_1 = 00110010011010110100110000010101 \\ 01011011101001010100111000010100.$$

Aplicando a troca T dos blocos de 32 dígitos dos lados esquerdo e direito temos:

$$T(N_1) = N_1' = 0101101110100101 \\ 01001110000101000011001 \\ 01101011010011000001010 1.$$

Para finalizar a criptografia vamos aplicar a permutação I^{-1} na seqüencia anterior:

$$C = I^{-1}(N_1') = 101011000011010111 \\ 01101000110110011010011000010 \\ 10011011010000000.$$

Logo essa seqüencia, é a mensagem criptografada. Assim o emissor A envia essa mensagem para o receptor B.

Para decifrar a seqüência recebida o receptor B deverá proceder de modo análogo ao processo de criframento.
O receptor B aplicará a função I a partir da Tabela 3, que é a primeira fase, e obterá a seqüência a seguir:

$$I(C) = 01011011101001010100111000010100 \\ 00011001001101011010011000001010 1.$$

Separando a seqüência anterior em blocos de 32 bits, obtemos dois blocos. Chamaremos os primeiros 32 bits de bloco da "esquerda", que denotaremos por "E_0" e os outros 32 bits restantes de bloco da "direita", que será denotado por "D_0":

$$E_0 = 01011011101001010100111000010100$$
$$D_0 = 00110010011010110100110000010101$$

Para o bloco D_0 faremos a expansão usando a Tabela 5. Assim, a seqüência de 32 bits será transformada em uma nova seqüência com 48 bits:

$$X(C) = 110110001101000010010 10 \\ 10100001100111001011010 01.$$

Usando a mesma chave K_1 de 48 bits que usamos para cifrar a mensagem, dada a seguir:

$$K_1 = 111101101010010010100010000110010110100111010001,$$

Fazemos a soma binária desses 48 bits com o bloco da direita D_0 e obtemos uma nova seqüência:

$$X(C) + K_1 = 001011100111010000110110010110100101000010111000.$$

Utilizando as Caixas S e fazendo os mesmos procedimentos adotados no ciframento, separemos a seqüência em blocos de 6 bits:

$$B_1 = 001011 \quad B_2 = 100111$$
$$B_3 = 010000 \quad B_4 = 110110$$
$$B_5 = 010110 \quad B_6 = 100101$$
$$B_7 = 000010 \quad B_8 = 111000$$

Teremos a seguinte redução de 6 bits para 4 bits dada a seguir: $B'_1 = 0011, B'_2 = 1001$, $B'_3 = 1101$, $B'_4 = 1010$, $B'_5 = 0100$, $B'_6 = 0101$, $B'_7 = 0110$, $B'_8 = 0000$. Juntando todos os blocos B'_i, para $i = 1, 2, ...8$, em uma só seqüência obtemos:

$$S = 00111001110110100100010101100000.$$

Usando a Tabela 6, da função permutação, na seqüência acima obtemos a seqüência a seguir no qual chamaremos de D_1:

$$P(S) = 011100000100001110000111101011 00.$$

Fazendo a soma binária de $E_0 + P(S)$ temos:

$$D_1 = E_0 + P(S) = 0010101111100101101001100110111000.$$

Juntando, respectivamente, as seqüências D_0 e D_1 temos:

$$N_1 = 00110010011010110100110000010100101011111001101100100110111000.$$

Aplicando T:

$$T(N_1) = N'_1 = 0010101111100110110010011011000001100100111000.$$

Para finalizar o deciframento vamos aplicar a função I^{-1} na seqüência anterior chegando em:

$$M = I^{-1}(N'_1) = 0011110000100101100000100111011001001001111000.$$

Logo, essa seqüência, é a mensagem decifrada. Ou seja, separando essa seqüência em blocos de 6 bits e passando para a base decimal, obtemos os números:

$$15\ 10\ 22\ 10\ 29\ 36\ 39\ 37\ 37\ 45,$$

que corresponde a mensagem original $FAMAT\_2008$.

Nesse exemplo, para simplificar, usamos uma única rodada, mas isso é inseguro. Para oferecer maior segurança e resistência à criptoanálise o ideal é que se realizem várias rodadas, no caso 16 rodadas é o tamanho típico para a criptografia DES.

Observação: Tipicamente, na criptografia DES, há um procedimento algoritmo de geração das chaves $K_1, ..., K_{16}$ a partir de uma única chave K fornecida pelos comunicantes. Neste trabalho não abordamos tal algoritmo. No entanto, o leitor interessado pode encontrá-lo em [9].

4 Discussão e Conclusões

Os modernos sistemas de criptografia consistem da principal aplicação de Teoria dos Números, mais especificamente, congruências e números primos. O estudo de números primos é quase tão antigo quanto a própria

matemática e teve origem com os antigos gregos. Não obstante, seu estudo ainda é extremamente ativo nos dias atuais, principalmente com o uso de recursos computacionais, e muita pesquisa tem sido desenvolvida por brilhantes matemáticos. O fato da segurança de todo sistema de troca de informações sigilosas estar baseado na dificuldade em se fatorar um número composto é, no mínimo, curioso, uma vez que o conceito de fatoração em números primos é algo do conhecimento geral de qualquer estudante de ensino fundamental. Mais curioso ainda é o fato de, mesmo com todo recurso tecnológico e computacional disponível, não existir um algoritmo de fatoração de números compostos grandes que seja pelo menos "semi-eficiente".

A história do ciframento e deciframento da mensagens é, assim como o estudo de números primos, bastante antiga e, sempre houve momentos em que os criadores de crifras estavam à frente dos "quebradores" de cifras e viceversa. Mesmo em épocas recentes, como na Segunda Guerra Mundial, temos exemplos de cifras que foram quebradas, [8] . No entanto, a partir da década de 1970, com o surgimento da Criptografia *RSA* e dos diversos sistemas criptográficos dele derivados ou nele inspirados, como o ElGamal e Rabin, parece que os cifradores estão à frente dos quebradores de cifras.

Referências

[1] Coutinho, S. C. *Números Inteiros e Criptografia RSA.* Rio de Janeiro, RJ: IMPA - SBM. Série de Computação e Matemática. 1997.

[2] Domingues, H. H. *Álgebra Moderna.* São Paulo, SP: Atual Editora. 1982.

[3] Domingues, H. H. *Fundamentos de Aritmética.* São Paulo, SP: Atual Editora. 1991.

[4] Lucchesi, C. L. *Introdução à Criptografia Computacional.* Campinas-SP: Editora da Unicamp. 1986.

[5] Mollin, R. A. *An Introduction to Cryptography.* New York: Chapman & Hall. 2001.

[6] Rivest, M,; Shamir, A. & Adleman, L. "A method for obtaining digital signatures and public-key cryptosystems". *Comm. ACM,* 21 (1978), 120-126.

[7] Santos, J. P. O. *Introdução à Teoria dos Números.* Rio de Janeiro, RJ: Publicação do Inst. de Mat. Pura e Aplicada (IMPA). Coleção Matemática Universitária. 1998.

[8] Singh, S. *O Livro dos Códigos.* Rio de Janeiro: Editora Record. 2001.

[9] Stallings, W. *Criptografia e Segurança de Redes.* 4ª. ed. São Paulo: Peason Prentice Hall. 2007.