Criptografia, assinaturas digitais e senhas segmentadas

Adriele Giareta Biase
Universidade Federal de Uberlândia - Faculdade de Matemática
Graduanda em Matemática - PROMAT
adrielegbiase@yahoo.com.br

Edson Agustini
Universidade Federal de Uberlândia - Faculdade de Matemática
Professor Associado I
agustini@ufu.br

Resumo: Este trabalho é uma exposição dos resultados básicos envolvendo Criptografia *RSA*. Sua base teórica é encontrada na Teoria dos Números, mais precisamente, na manipulação de máximos divisores comuns, fatorações, congruências e métodos para determinar números primos. A Criptografia *RSA* é composta por duas fases: ciframento e deciframento, nas quais utilizamos $n = pq$, com p e q números primos muito grandes. A segurança da Criptografia *RSA* baseia-se na dificuldade de fatorar n para obter p e q, que são números muito grandes. Além da Criptografia *RSA*, os pré-requisitos de Teoria dos Números são expostos nesse trabalho, assim como aplicações em senhas segmentadas e assinaturas digitais.

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.

Criptografia é o estudo de métodos para cifrar (ou modificar) uma mensagem a ser enviada de tal forma que apenas o receptor legítimo consiga interpretá-la. A base matemática da criptografia moderna 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) [5], ao qual daremos ênfase nesse trabalho. Para implementar esse método, precisamos escolher dois números primos muito grandes p e q e, na fase de ciframento de uma mensagem, usamos $n = pq$. Já, para o deciframento da mensagem, precisamos conhecer p e q. A segurança do método está justamente na dificuldade de fatorar n, que é público, para obter p e q, que são privados.

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 do algoritmo da Criptografia *RSA*, a demonstração de sua funcionalidade e uma aplicação em assinaturas digitais. Além disso, uma aplicação de sistemas lineares de congruências é abordado: as senhas segmentadas que, embora não use criptografia, ilustra o quanto as congruências podem ser úteis no processo de segurança de informações e valores.

Em decorrência do exposto, o trabalho está esquematizado em três grandes partes:

- Principais preliminares da Teoria dos Números e algoritmos necessários à compreensão da Criptografia *RSA*.
- Processo de ciframento e deciframento de mensagens utilizando a Criptografia *RSA*.
- Aplicações em assinaturas digitais e senhas segmentadas.

2 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 resolver um dado problema. As proposições apresentadas nessa seção são básicas e suas demonstrações podem ser encontradas em livros introdutórios de Teoria dos Números como, por exemplo, [1], [2] , [3] e [6] .

2.1 Alguns Teoremas e Algoritmos Importantes

O Teorema da Divisão de Inteiros

Proposição (*Teorema de Eudoxius*) Dados a e b inteiros com $b \neq 0$ então a é um múltiplo de b ou se encontra entre dois múltiplos consecutivos de b, isto é, correspondendo a cada par de inteiros a e $b \neq 0$ existe um inteiro q tal que, para $b > 0$,

$$qb \leq a < (q+1)b$$

e para $b < 0$,

$$qb \leq a < (q-1)b$$

Teorema (*da Divisão de Inteiros*) Sejam $a, b \in \mathbb{Z}$, $b > 0$. Então, existem únicos $q, r \in \mathbb{Z}$, $0 \leq r < b$, tais que

$$a = bq + r.$$

Demonstração.

Pelo Teorema de Eudoxius, como $b > 0$, existe q satisfazendo:

$$qb \leq a < (q+1)\, b.$$

Assim,

$$0 \leq a - qb$$

e

$$a < qb + b \Rightarrow a - qb < b.$$

Se definirmos $r = a - qb$, teremos garantido a existência de q e r.

Quanto à unicidade:

Vamos supor a existência de outro par q_1 e r_1, em que:

$$a = q_1 b + r_1$$

com $0 \leq r_1 < b$.
Temos:

$$qb + r - (q_1 b + r_1) = 0 \Rightarrow qb - q_1 b + r - r_1 = 0 \Rightarrow b(q - q_1) = r_1 - r \tag{1}$$

Mas como $r_1 < b$ e $r < b$ temos $|r_1 - r| < b$. Logo:

$$b\,|q - q_1| = |r_1 - r| \Rightarrow |q - q_1| = \frac{|r_1 - r|}{b} < 1 \Rightarrow |q - q_1| = 0 \Rightarrow q - q_1 = 0 \Rightarrow q = q_1.$$

De (1) temos:

$$b(q - q_1) = r_1 - r \Rightarrow b(q - q) = r_1 - r \Rightarrow 0 = r_1 - r \Rightarrow r_1 = r.$$

□

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

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

□

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:

$$\text{mdc}(a,b) = \text{mdc}\,(b,r_1) = \text{mdc}\,(r_1,r_2) = \cdots = \text{mdc}\,(r_{n-2},r_{n-1}) = \text{mdc}\,(r_{n-1},0) = r_{n-1},$$

devido ao Teorema de Euclides.

Teorema de Euclides Estendido e Algoritmo Euclidiano Estendido

Proposição. 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, $|d| \leq |n|$. □

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 $B = \{na + mb : m, n \in \mathbb{Z}\}$ o conjunto de todas as combinações lineares de a e b. 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:

$$r = a - qc = a - q(\alpha a + \beta b) = a - q\alpha a - q\beta b = (1 - q\alpha)\,a + (-q\beta)\,b.$$

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,

$$c = \alpha a + \beta b \Rightarrow c = \alpha\,(K_1 d) + \beta\,(K_2 d) \Rightarrow c = d\,(\alpha K_1 + \beta K_2)\,.$$

Logo $d \mid c$. Da proposição acima, temos que $d \leq c$ (ambos positivos) e como $d < c$ não é possível, uma vez que d é máximo divisor comum, então $c = d$.

Concluímos então que $d = \alpha a + \beta b$. □

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 mdc(a, b). Utilizando o Algoritmo Euclidiano, obtemos, a seqüência de divisões abaixo:

$$\begin{aligned} a &= bq_1 + r_1 \text{ e } r_1 = ax_1 + by_1 \\ b &= r_1q_2 + r_2 \text{ e } r_2 = ax_2 + by_2 \\ r_1 &= r_2q_3 + r_3 \text{ e } r_3 = ax_3 + by_3 \\ &\vdots \\ r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1} \text{ e } r_{n-1} = ax_{n-1} + by_{n-1} \\ r_{n-2} &= r_{n-1}q_n \text{e } r_n = 0 \end{aligned}$$

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}

TABELA 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 temos 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,

$$r_{j-2} = r_{j-1}q_j + r_j \Rightarrow r_j = r_{j-2} - r_{j-1}q_j \tag{2}$$

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

$$r_{j-1} = ax_{j-1} + by_{j-1} \text{ e } r_{j-2} = ax_{j-2} + by_{j-2}. \tag{3}$$

Substituindo (3) em (2), 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 $\beta = y_{n-1}$.

Fatoração

Proposição (*Teorema da Fatoração Única*) Dado um inteiro $n \geq 2$ podemos sempre escrevê-lo de modo único, na forma

$$n = p_1^{e_1} \dots p_k^{e_k},$$

sendo $1 < p_1 < p_2 < p_3 < \cdots < p_k$ números primos e $e_1, e_2, \dots, e_k$ inteiros positivos.

Demonstração.

Existência da Fatoração.
Tendo n como entrada, tentamos dividir n por cada um dos inteiros de 2 a $n-1$. Se algum destes inteiros dividir n, então achamos um fator de n. E, além disso, o menor fator p_1 que achamos desta maneira tem que ser primo. De fato, seja p_1 um inteiro tal que $2 \leq p_1 \leq n-1$. Suponhamos que p_1 seja o menor fator de n e que p_1' é um fator (maior do que 1) de p_1. Logo, existem inteiros a e b tais que

$$n = p_1 a;$$
$$p_1 = p_1' b.$$

Logo, $n = p_1' ab$. Portanto, p_1' também é um fator de n. Como supomos que p_1 é o menor fator de n, concluímos que $p_1 \leq p_1'$. Por outro lado, p_1' é fator de p_1 o que só pode acontecer se $p_1' \leq p_1$. Das duas desigualdades segue que $p_1 = p_1'$.
Assim o único fator de p_1 maior que 1 é o próprio p_1. Então, p_1 é primo.

Repetimos o procedimento descrito acima em $m_1 = \dfrac{n}{p_1}$ e encontramos um fator p_2 de m_1. Tomamos $m_2 = \dfrac{m_1}{p_2}$ e repetimos o procedimento para m_2, e assim por diante. Após um certo número i de etapas, encontramos $m_i = p_i$. Logo, $n = p_1 p_2 \dots p_i$. Juntando os $p_j's$ iguais em uma mesma base, podemos escrever $n = p_1^{e_1} \dots p_k^{e_k}$, como queríamos. □

Observações.

(1) Pelo Teorema da Fatoração Única, um algoritmo para fatorar n composto consiste em fazer uma busca de fatores de n começando por 2 e não precisamos passar de $n-1$, pois um número inteiro não pode ter um fator maior que ele próprio. Na verdade não precisamos procurar fatores maiores do que $\sqrt{n}$ pois o menor fator de n, maior que 1, é sempre menor do que ou igual a $\sqrt{n}$. De fato, seja $f > 1$ o menor fator de n. Então, existe um inteiro positivo a tal que $n = fa$. Como f é o menor fator, certamente

$$f \leq a \Rightarrow f^2 \leq fa \Rightarrow f^2 \leq n,$$

que é equivalente a $f \leq \sqrt{n}$.

(2) A demonstração do Teorema da Fatoração Única permite que elaboremos um algoritmo para encontrar um fator de um número inteiro positivo n:
Algoritmo da Fatoração
Etapa (1): Informe um inteiro positivo n.
Etapa (2): Comece com $f = 2$;

Etapa (3): Se $\frac{n}{f}$ é inteiro, então f é fator de n. Caso contrário, siga para a Etapa (4) .
Etapa (4): Aumente em f uma unidade e siga para a Etapa (5) .
Etapa (5): Se $f > \sqrt{n}$ então n é primo. Caso contrário, volte para o Etapa (3) .
Mesmo não encontrando um fator f de n, o algoritmo pára. De fato, aumentando f de uma unidade a cada ciclo, f irá superar o número $\sqrt{n}$ e, portanto, n será primo.

(3) É claro que o algoritmo de fatoração descrito acima é muito ineficiente quando estamos tentando fatorar números muito grandes. Abaixo iremos apresentar um algoritmo melhor para o caso de n ser composto por dois fatores primos (mesmo grandes) que não estejam muito distantes um do outro.

Algoritmo de Fermat

Proposição (*Teorema de Fermat*) Seja n natural ímpar. Então, $n = (x+y)(x-y) = x^2 - y^2$, com x, y números naturais, ou n é primo.

Demonstração.

Suponhamos que n é composto. Logo, n pode ser fatorado na forma $n = ab$, sendo $a \leq b$. Vamos obter naturais x e y tais que $n = x^2 - y^2$. Suponhamos que existam os naturais x e y. Logo:

$$n = ab = (x+y)(x-y) = x^2 - y^2.$$

Como $x - y \leq x + y$, isto sugere que tomemos

$$\begin{cases} a = x - y \\ b = x + y \end{cases} \iff \begin{cases} b + a = 2x \\ b - a = 2y \end{cases} \iff \begin{cases} x = \dfrac{b+a}{2} \\ \\ y = \dfrac{b-a}{2} \end{cases}.$$

Mas n é ímpar, então a e b são ímpares (pois $n = ab$). Logo, $b+a$ e $b-a$ são pares, conseqüentemente $\frac{b+a}{2}$ e $\frac{b-a}{2}$ são inteiros, ou seja x e y são números naturais. Conclusão: se n for composto, então existem x e y naturais tais que $n = x^2 - y^2$. □

O *Algoritmo de Fermat* é utilizado para encontrar dois fatores a e b de um número natural n ímpar composto.
Esse algoritmo será eficiente quando n tiver um fator primo que não seja muito menor que$\sqrt{n}$.
Adotemos $\lfloor x \rfloor$, x real positivo, como sendo a parte inteira de x.

As etapas do algoritmo são:
(i) Comece com $x = \lfloor \sqrt{n} \rfloor$. Se $n = x^2$, então x é fator de n e podemos parar.
(ii) Caso contrário, aumente x de uma unidade e calcule $y = \sqrt{x^2 - n}$.
(iii) Repita a Etapa 2 até encontrar um valor inteiro para y, ou até que x seja igual a $\frac{n+1}{2}$. No primeiro caso, n tem fatores $x - y$ e $x + y$, no segundo, n é primo.

Se $n = ab$ é ímpar composto, pelo Teorema de Fermat, existem números naturais

$$x = \frac{b+a}{2} \text{ e } y = \frac{b-a}{2}$$

tais que $n = x^2 - y^2$. Encontrando esses valores temos:

$$n = x^2 - y^2 = (x+y)(x-y),$$

ou seja, $a = x + y$ e $b = x - y$ são fatores de n.

Se n é primo, então só podemos ter $a = 1$ e $b = n$. Com isto, $x = \dfrac{n+1}{2}$ e isto justifica a parada do algoritmo na Etapa (iii).

Voltemos ao caso em que $n = ab$ é composto.
Se $a = b$, o algoritmo obtém a resposta desejada na Etapa (i) pois

$$x = \lfloor \sqrt{n} \rfloor = \lfloor \sqrt{aa} \rfloor = \left\lfloor \sqrt{a^2} \right\rfloor = a$$

e fatoramos n.

Se $a \neq b$, podemos supor que

$$1 < a < b < n.$$

Veremos que, neste caso, o algoritmo vai parar se forem satisfeitas as desigualdades:

$$\lfloor \sqrt{n} \rfloor \leq \frac{a+b}{2} < \frac{n+1}{2}. \tag{4}$$

Provando a desigualdade da direita:

$$1 < b \Rightarrow 1\,(a-1) < b(a-1) \Rightarrow a - 1 + b - b < ab - b + 1 - 1 \Rightarrow$$
$$a + b - (b+1) < n + 1 - (b+1) \Rightarrow a + b < n + 1 \Rightarrow \frac{a+b}{2} < \frac{n+1}{2}.$$

Considerando agora a desigualdade da esquerda:
Sabemos que $\lfloor \sqrt{n} \rfloor \leq \sqrt{n}$. Logo,

$$\frac{(b+a)^2}{4} - \frac{(b-a)^2}{4} = ab = n \Rightarrow \frac{(b+a)^2}{4} - n = \frac{(b-a)^2}{4} \Rightarrow \frac{(b+a)^2}{4} - n \geq 0 \Rightarrow$$
$$n \leq \frac{(b+a)^2}{4} \Rightarrow \sqrt{n} \leq \frac{a+b}{2} \Rightarrow \lfloor \sqrt{n} \rfloor \leq \frac{a+b}{2}.$$

No algoritmo, a variável x é iniciada com o valor $\lfloor \sqrt{n} \rfloor$ e vai sendo aumentada de uma unidade até encontrar um inteiro $y = \sqrt{x^2 - n}$. Assim, (4) nos garante que, se n for composto, chegaremos a $\dfrac{a+b}{2}$ antes de chegar a $\dfrac{n+1}{2}$. Quando $x = \dfrac{a+b}{2}$, então $y = \sqrt{\left(\dfrac{a+b}{2}\right)^2 - ab} = \dfrac{b-a}{2}$ e o algoritmo pára, e obtemos os fatores $a = x + y$ e $b = x - y$ de n.

Exemplo

Tomemos $n = 281675$. Aplicando o Algoritmo de Fermat temos:

Comecemos com $x = \lfloor \sqrt{n} \rfloor = \left\lfloor \sqrt{281675} \right\rfloor = 530$.
Mas $x^2 = (530)^2 = 280900 < 281675$. Logo, devemos somar em x uma unidade, até encontrarmos um valor para $y = \sqrt{x^2 - n}$ que seja inteiro, ou até que x seja igual a $\dfrac{n+1}{2}$. Para isso, vamos construir uma tabela:

x	$y = \sqrt{x^2 - n}$
531	$16,911535$
532	$36,728735$
533	$49,132474$
534	59

Ao desenvolver a quarta linha obtivemos um y inteiro. Portanto, $x = 534$ e $y = 59$. Logo, os fatores de n são: $a = x + y = 593$ e $b = x - y = 475$.

Observação. Não basta escolher primos grandes para garantir que n seja difícil de fatorar, pois se escolhermos primos grandes e muito próximos um do outro, então n é facilmente fatorado pelo Algorimo de Fermat. De fato, seja $n = ab$. Se $a \approx b$, temos

$$y = \frac{b-a}{2} \Rightarrow y \approx 0 \qquad \text{e} \qquad x = \frac{b+a}{2} \Rightarrow x \approx a$$

Como $n = x^2 - y^2 \Rightarrow n \approx x^2 \Rightarrow \sqrt{n} \approx x$, ou seja, são necessários poucas etapas para que o Algoritmo de Fermat forneça os fatores de n.

2.2 Congruências

Aritmética Modular

A seguir, delineamos alguns conceitos de aritmética modular, a base para o desenvolvimento da criptografia moderna. Começamos com a noção de relação de equivalência.
Uma relação binária $\sim$ sobre um conjunto X não vazio é chamada relação de equivalência sobre X, quando satisfaz as três seguintes propriedades:

(1) $x \sim x$; (reflexiva)
(2) Se $x \sim y$, então $y \sim x$; (simétrica)
(3) Se $x \sim y$ e $y \sim z$, então $x \sim z$. (transitiva)

Uma relação binária permite compararmos dois elementos de um conjunto segundo uma dada regra. As relações de equivalência são usadas para classificar os elementos de um conjunto em subconjuntos com propriedades semelhantes denominados classes de equivalência. A classe de equivalência de um elemento $x \in X$ é denotada por

$$\overline{x} = \{y \in X : y \sim x\}.$$

Temos ainda que qualquer elemento de uma classe de equivalência é um representante de toda a classe. Destacamos ainda dois resultados muito importantes relacionados ao conjunto X com a relação de equivalência $\sim$:

(1) X é a união de todas as classes de equivalência.
(2) A intersecção de duas classes de equivalência distintas é vazia.

Uma relação de equivalência no conjunto dos números inteiros pode ser construída do seguinte modo: dois inteiros a e b, cuja diferença é um múltiplo de um $n \in \mathbb{N}^*$, são ditos congruentes módulo n se $a - b$ é múltiplo de n e são denotados por $a \equiv b (\mathrm{mod}\, n)$.
Mostremos que a congruência módulo n é uma relação de equivalência:

Sejam $a, b, c \in \mathbb{Z}$, então:
(i) $a \equiv a (\mathrm{mod}\, n)$. De fato, $a - a = 0n$.
(ii) $a \equiv b (\mathrm{mod}\, n) \Longrightarrow b \equiv a (\mathrm{mod}\, n)$. De fato,

$$a - b = kn \text{ e}$$

$$b - a = -(b - a) = -kn \Longrightarrow b \equiv a (\mathrm{mod}\, n); k \in \mathbb{Z}.$$

(iii)

$$a \equiv b (\mathrm{mod}\, n),\ b \equiv c (\mathrm{mod}\, n) \Longrightarrow a \equiv c (\mathrm{mod}\, n).$$

De fato, $a-b=k_1n$ e $b-c=k_2n$. Como $(a-b)+(b-c)=a-c$, temos

$$(k_1n)+(k_2n)=a-c \Rightarrow a-c=(k_1+k_2)n,$$

ou seja, $a \equiv c(\mathrm{mod}\, n)$; $k_1, k_2 \in \mathbb{Z}$.

O conjunto de todas as classes de equivalência da relação de congruência módulo n em $\mathbb{Z}$ é denotado por $\mathbb{Z}_n$ e denominado conjunto dos inteiros módulo n. Dessa forma, a classe de equivalência de a é dada por $\overline{a}=\{a+kn : k \in \mathbb{Z}\}$. Se $a \in \mathbb{Z}$, então podemos dividi-lo por n, obtendo q e r inteiros, tais que $a=nq+r$ e $0 \leq r < n$. Daí, $a-r=nq$, que é múltiplo de n e, então, $a \equiv r(\mathrm{mod}\, n)$. Logo, qualquer inteiro é congruente módulo n a um inteiro entre 0 e $n-1$. Assim, os elementos do conjunto quociente de $\mathbb{Z}$ na relação de congruência módulo n são: $\overline{0}, \overline{1}, ..., \overline{n-1}$. Esse conjunto é assim denotado:

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

Podemos utilizar congruência para calcular o resto da divisão de uma potência por um número qualquer. Vejamos um exemplo: calcular o resto da divisão de 10^{135} por 7. Para efetuar esse calculo, consideremos o *Pequeno Teorema de Fermat.*

Teorema (*Pequeno Teorema de Fermat*) Se $p > 1$ é um número primo que não divide o inteiro a, então:

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

Assim, pelo resultado acima,

$$10^6 \equiv 1(\mathrm{mod}\, 7).$$

Como $135 = 6.22 + 3$, temos:

$$10^{135} \equiv (10^6)^{22}10^3 \equiv 1^{22}10^3 \equiv 6(\mathrm{mod}\, 7).$$

Logo, o resto da divisão de 10^{135} por 7 é 6.

Nem sempre é tão simples fazer esses cálculos, já que é raro encontramos uma potência que seja congruente a 1, no módulo n. Para tanto, lançamos mão de um método para o cálculo do resto da divisão de uma potência por um número. Esse método é conhecido como *Método dos Quadrados Repetidos* e será apresentado adiante.

Equações Diofantinas

Chamamos de *equação diofantina* a uma equação polinomial (com qualquer número de incógnitas), com coeficientes inteiros. Em uma equação diofantina, interessa apenas soluções inteiras.
Esses tipos de equações foram abordados pelo matemático grego Diofanto em seu tratado *Aritmética*, escrito por volta de 250 *d.C*. Daí o fato das equações serem chamadas de *diofantinas.*

Proposição. Se $\mathrm{mdc}(a,b)=d$, então $\mathrm{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demonstração.

Pelo *Teorema de Euclides Estendido,* $\mathrm{mdc}(ta, tb)$ é o menor valor positivo de $mtb+ntb$ (m e n inteiros), que é igual a t vezes o menor valor positivo de $ma+nb = t\,\mathrm{mdc}(a,b)$.
Como a e b são divisíveis por c, temos que $\frac{c}{a}$ e $\frac{c}{b}$ são inteiros. Basta, então substituir a por $\frac{c}{a}$ e b por $\frac{c}{b}$, tomando $t=c$.

No que acabamos de descrever c é um divisor comum de a e b. Se tomarmos c como sendo o máximo divisor comum d, teremos o resultado desejado. □

Proposição. Se a, b, c, m e n são inteiros $c \mid a$ e $c \mid b$, então $c \mid (ma + mb)$.

Demonstração.

Se $c \mid a$, então

$$a = K_1 c \Rightarrow am = mK_1 c.$$

Se $c \mid b$, então

$$b = K_2 c \Rightarrow bn = nK_2 c.$$

Somando as equações acima:

$$am + bn = mK_1 c + nK_2 c \Rightarrow am + bn = c\left(mK_1 + nK_2\right).$$

Logo, $c \mid (am + bn)$. □

Proposição. Se $a \mid bc$ e $\text{mdc}(a, b) = 1$, então $a \mid c$.
Demonstração.

Como $\text{mdc}(a, b) = 1$, pelo Teorema de Euclides Estendido, existem n e m tais que

$$na + mb = 1 \Rightarrow n(ac) + m(bc) = c.$$

Como $a \mid ac$ e, pela hipótese, $a \mid bc$, então $a \mid c$. □

Teorema. (*Solução geral de equação diofantina linear com duas incógnitas*) Sejam a e b inteiros positivos e $d = \text{mdc}(a, b)$. Se $d \nmid c$, então a equação diofantina

$$ax + by = c$$

não possui nenhuma solução inteira. Se $d \mid c$ ela possui infinitas soluções e se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções são dadas por:

$$x = x_0 + \left(\frac{b}{d}\right)k \qquad \text{e} \qquad y = y_0 - \left(\frac{a}{d}\right)k$$

com $k \in \mathbb{Z}$.

Demonstração.

Se $d \nmid c$, então a equação $ax + by = c$, não possui solução pois, como $d \mid a$ e $d \mid b$, d deveria dividir c, o qual é uma combinação linear de a e b. Suponha que $d \mid c$. Pelo Teorema de Euclides Estendido, existem inteiros n_0 e m_0, tais que:

$$an_0 + bm_0 = d.$$

Como $d \mid c$, existe um inteiro k tal que $c = kd$. Se multiplicarmos a equação acima por k, teremos:

$$a(n_0 k) + b(m_0 k) = kd = c,$$

então

$$x_0 = (n_0 k) \qquad \text{e} \qquad y_0 = (m_0 k)$$

é uma solução de

$$ax + by = c.$$

A verificação de x e de y é trivial. Se

$$x = x_0 + \left(\frac{b}{d}\right)k \qquad \text{e} \qquad y = y_0 - \left(\frac{a}{d}\right)k$$

são soluções, temos

$$ax + by = a\left(x_0 + \left(\frac{b}{d}\right)k\right) + b\left(y_0 - \left(\frac{a}{d}\right)k\right) = ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k = ax_0 + by_0 = c.$$

O que acabamos de encontrar é apenas uma solução particular (x_0, y_0) e, a partir dela, podemos gerar infinitas soluções. Vamos mostrar agora que toda solução da equação $ax + by = c$ é da forma acima. Suponhamos que (x, y) seja uma solução, ou seja, $ax+by = c$. Como $ax_0+by_0 = c$, então se subtrairmos as duas equações, obtemos:

$$ax + by - ax_0 - by_0 = a(x - x_0) + b(y - y_0) = 0,$$

o que implica

$$a(x - x_0) = b(y_0 - y).$$

Pela hipótese $d = \text{mdc}(a, b)$, logo, $\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.
Portanto, dividindo os dois menbros da última igualdade por d, temos:

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y).$$

Logo, $\left(\frac{b}{d}\right) \mid (x - x_0)$ e, portanto, existe um inteiro k satisfazendo

$$x - x_0 = k\left(\frac{b}{d}\right), \quad \text{ou seja:} \quad x = x_0 + \left(\frac{b}{d}\right)k$$

Substituindo:

$$\frac{a}{d}\left(x_0 + \left(\frac{b}{d}\right)k - x_0\right) = \frac{b}{d}(y_0 - y) \Rightarrow \frac{a}{d}k = (y_0 - y) \Rightarrow y = y_0 - \left(\frac{a}{d}\right)k.$$

□

Sistema de Equações Diofantinas Lineares

Proposição. Se a, b, c e m são inteiros e $ac \equiv bc \pmod m$, então $a \equiv b \pmod m$ sendo $d = \text{mdc}(c, m)$.

Demonstração.

De $ac \equiv bc \pmod m$ temos $ac - bc = c(a - c) = km$. Se dividirmos os dois membros por d, teremos $\left(\frac{c}{d}\right)(a - c) = k\left(\frac{m}{d}\right)$. Logo, $\frac{m}{d} \mid (a - d)$ o que implica

$$a \equiv b \left(\mod \frac{m}{d}\right).$$

□

Proposição. Se a e b são inteiros, então $a \equiv b \pmod m$ se, e somente se, existir um inteiro k tal que $a = b + km$.

Demonstração.

($\Rightarrow$) Se $a \equiv b \pmod{m}$, então $m \mid (a-b)$ o que implica na existência de um inteiro k tal que $a-b = km$, isto é, $a = b + km$.

($\Leftarrow$) Se k satisfaz $a = b + km$, temos

$$km = a - b,$$

ou seja, que $m \mid (a-b)$ isto é,

$$a \equiv b (\mathrm{mod}\, m).$$

□

Proposição. Se a, b, c e m são inteiros e $ac \equiv bc \pmod{m}$, então $a \equiv b \left(\mathrm{mod}\, \frac{m}{d}\right)$ sendo $d = \mathrm{mdc}(c, m)$

Demonstração.

De $ac \equiv bc \pmod{m}$ tiramos que $ac - bc = c(a-b) = km$. Se dividirmos os dois membros por d, temos $\left(\frac{c}{d}\right)(a-b) = k\left(\frac{m}{d}\right)$. Logo

$$\left(\frac{m}{d}\right) \Big| \left(\frac{c}{d}\right)(a-b)$$

e como $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$, temos

$$\left(\frac{m}{d}\right) \Big| (a-b)$$

o que implica

$$a \equiv b \left(\mathrm{mod}\, \frac{m}{d}\right).$$

□

Proposição. Se $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ..., $a \equiv b \pmod{m_r}$ sendo $a, b, m_1, m_2, ..., m_r$ são inteiros com m_i positivos, $i = 1, 2, 3, ..., r$, então

$$a \equiv b (\mathrm{mod}\, [m_1, m_2, m_3, ..., m_r]),$$

sendo $[m_1, m_2, m_3, ..., m_r]$ o mínimo múltiplo comum de $m_1, m_2, m_3, ..., m_r$.

Demonstração.

Seja p_n o maior primo que aparece nas fatorações de $m_1, m_2, m_3, ..., m_r$. Cada m_i, $i = 1, 2, 3, ..., r$ pode, então, ser expresso como

$$m_i = p_1^{\alpha_{1i}} p_1^{\alpha_{2i}} \dots p_n^{\alpha_{ni}}.$$

(alguns α_{ji} podem ser nulos).
Como $m_i \mid (a-b)$, $i = 1, 2, 3, ..., r$, temos $p_n^{\alpha_{ji}} \mid (a-b)$, $i = 1, 2, 3, ..., r$ e $j = 1, 2, 3, ..., r$. Logo, se tomarmos $\alpha_j = \max_{1 \le i \le r} \{\alpha_{ji}\}$ teremos

$$p_1^{\alpha_1} p_1^{\alpha_2} \cdots p_n^{\alpha_n} \mid (a-b).$$

Mas,

$$p_1^{\alpha_1} p_1^{\alpha_2} \cdots p_n^{\alpha_n} = [m_1, m_2, m_3, ..., m_r],$$

o que implica

$$a \equiv b (\mathrm{mod}\, [m_1, m_2, m_3, ..., m_r]).$$

□

Proposição. Sejam a, b e m inteiros tais que $m > 0$ e $\text{mdc}\,(a, m) = d$. No caso em que $d \nmid b$ a congruência $ax \equiv b \,(\text{mod}\, m)$ não possui nenhuma solução e quando $d \mid b$, possui exatamente d soluções incogruentes módulo m.

Demonstração.

Sabemos que o inteiro x é solução de $ax \equiv b \,(\text{mod}\, m)$ se, e somente se, existe um inteiro y tal que $ax = b + my$, ou, o que é equivalente, $ax - my = b$. Sabemos também que esta equação não possui nenhuma solução caso $d \nmid b$, e que se $d \mid b$ ela possui infinitas soluções dadas por

$$x = x_0 - \left(\frac{m}{d}\right) k \text{ e } y = y_0 - \left(\frac{a}{d}\right) k,$$

sendo que (x_0, y_0) é uma solução particular de $ax - my = b$. Logo, a congruência $ax \equiv b \,(\text{mod}\, m)$ possui infinitas soluções dadas por $x = x_0 - \left(\frac{m}{d}\right) k$. Como estamos interessados em saber o número de soluções incongruentes, vamos tentar descobrir sob que condições $x_1 = x_0 - \left(\frac{m}{d}\right) k_1$ e $x_2 = x_0 - \left(\frac{m}{d}\right) k_2$ são congruentes módulo m. Se x_1 e x_2 são congruentes, então

$$x_0 - \left(\frac{m}{d}\right) k_1 \equiv x_0 - \left(\frac{m}{d}\right) k_2 \,(\text{mod}\, m)\,.$$

Isto implica

$$\left(\frac{m}{d}\right) k_1 \equiv \left(\frac{m}{d}\right) k_2 \,(\text{mod}\, m)\,,$$

e como $\frac{m}{d} \Big| \frac{m}{d}$, o que nos permite o cancelamento de $\frac{m}{d}$, temos $k_1 \equiv k_2 \,(\text{mod}\, d)$.
Observemos que m foi substituído por

$$d = \frac{m}{\frac{m}{d}}.$$

Isto nos mostra que soluções incongruentes serão obtidas ao tomarmos

$$x = x_0 - \left(\frac{m}{d}\right) k,$$

onde k percorre um sistema completo de resíduos módulo d, o que conclui a demonstração. □

Teorema. (*Resto Chinês*) Sejam $m_1, m_2, m_3, ..., m_r$ números inteiros maiores que zero e tais que $\text{mdc}\,(m_i, m_j) = 1$, sempre que $i \neq j$. Façamos

$$m = m_1 m_2 m_3 ... m_r$$

e sejam $b_1, b_2, b_3, ..., b_r$, respectivamente, soluções das congruências lineares

$$\frac{m}{m_j} y \equiv 1 (\text{mod}\, m_j), \text{ sendo } j = 1, 2, 3, ..., r.$$

Então o sistema

$$\begin{cases} x \equiv a_1 (\text{mod}\, m_1) \\ x \equiv a_2 (\text{mod}\, m_2) \\ x \equiv a_3 (\text{mod}\, m_3) \\ \qquad \vdots \\ x \equiv a_r (\text{mod}\, m_r) \end{cases}$$

possui solução e a solução é única módulo m, sendo $m = m_1 m_2 m_3 ... m_r$.

Demonstração.

Do fato, de $\text{mdc}(1, m_i) = 1$, temos que $x \equiv a_i \,(\text{mod}\, m_i)$ possui uma única solução que denotaremos por b_i. Se definirmos $y_i = \dfrac{m}{m_i}$ sendo $m = m_1 m_2 m_3 ... m_r$, teremos $\text{mdc}\,(y_i, m_i) = 1$, uma vez que $\text{mdc}\,(m_i, m_j) = 1$ para $i \neq j$. Assim, temos a garantia de que cada uma das conguências $y_i x \equiv 1(\text{mod}\, m_i)$ possui uma única solução que denotaremos por $\overline{y}_i$. Logo,

$$y_i \overline{y}_i \equiv 1 \,(\text{mod}\, m_i)\,,\ i = 1, 2, 3, ..., r.$$

Afirmamos que o número x dado por

$$x = b_1 y_1 \overline{y_1} + b_2 y_2 \overline{y_2} + b_3 y_3 \overline{y_3} + \cdots + b_r y_r \overline{y_r}$$

é uma solução para o sistema de congruências. De fato:

$$x = a_i b_1 y_1 \overline{y_1} + a_i b_2 y_2 \overline{y_2} + \cdots + a_i b_r y_r \overline{y_r} \equiv a_i b_i y_i \overline{y_i} (\text{mod}\, m_i) \equiv a_i b_i \equiv c_i (\text{mod}\, m_i)$$

uma vez que y_j é divisível por m_i, para $i \neq j, y_i \overline{y_i} \equiv 1 (\text{mod}\, m_i)$, e b_i é solução de $x \equiv a_i (\text{mod}\, m_i)$.

Quanto à unicidade, temos que esta solução deve ser única, módulo m. Se $\overline{x}$ é uma outra solução para o nosso sistema, então $\overline{x} \equiv a_i \equiv x (\text{mod}\, m_i)$ e, sendo $\text{mdc}\,(m_i, m_j) = 1$, obtemos $\overline{x} \equiv x (\text{mod}\, m_i)$. Logo, $m_i \mid (\overline{x} - x)\,,\ i = 1, 2, 3, ..., r$. Mas, como $\text{mdc}\,(m_i, m_j) = 1$ para $i \neq j$ temos que

$$[m_1, m_2, m_3, ..., m_r] = m_1 m_2 m_3 ... m_r.$$

Portanto, $m_1 m_2 m_3 ... m_r \mid (\overline{x} - x)$, ou seja $\overline{x} \equiv x (\text{mod}\, m)$, o que conclui a demonstração. □

Algoritmo do Teorema do Resto Chinês.

Etapa 1: Faça $m = m_1 m_2 m_3 ... m_r$ e passe para a etapa seguinte.
Etapa 2: Faça $y_1 = \dfrac{m}{m_1}$, $y_2 = \dfrac{m}{m_2}$, $y_3 = \dfrac{m}{m_3}$, $\cdots$, $y_r = \dfrac{m}{m_r}$ e passe para a Etapa 3.
Etapa 3: Para $i = 1, 2, 3, ..., r$ resolva as equações:

$$y_i x = 1 \,(\text{mod}\, m_i)$$

e chame de $\overline{y_i} = x$, sendo $0 \leq x < m_i$.
Etapa 4: Faça

$$x \equiv c_1 y_1 \overline{y_1} + c_2 y_2 \overline{y_2} + c_3 y_3 \overline{y_3} + \cdots + c_r y_r \overline{y_r} \,(\text{mod}\, m_1 m_2 m_3 ... m_r)\,.$$

□

2.3 Algoritmos para o Cálculo de $a^e \,(\text{mod}\, n)$

Método dos Quadrados Repetidos

Como dito anteriormente, o objetivo desse método é calcular a congruência de b^r módulo 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.
Encontremos a tal que $a \equiv b^r \pmod{n}$, sendo $b = 227, r = 106$ e $n = 451$.

Solução.
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 $d \equiv 1.115 \pmod{451} \Rightarrow$
$\Rightarrow d = 115 \Rightarrow c = 115$

Para $j = 2$
$b_2 \equiv 115^2 \pmod{451} \Rightarrow b_2 = 146$
$a_2 = 0 \Rightarrow c = 115$

Para $j = 3$
$b_3 \equiv 146^2 \pmod{451} \Rightarrow b_3 = 119$
$a_3 = 1$, então $d \equiv 115.119 \pmod{451} \Rightarrow$
$\Rightarrow d = 20 \Rightarrow c = 20$

Para $j = 4$
$b_4 \equiv 119^2 \pmod{451} \Rightarrow b_4 = 180$
$a_4 = 0 \Rightarrow c = 20$

Para $j = 5$
$b_5 \equiv 180^2 \pmod{451} \Rightarrow b_5 = 379$
$a_0 = 1 \Rightarrow d \equiv 20.379 \pmod{451} \Rightarrow$
$\Rightarrow d = 364 \Rightarrow c = 364$

Para $j = 6$
$b_6 \equiv 379^2 \pmod{451} \Rightarrow b_6 = 223$
$a_6 = 1 \Rightarrow d \equiv 364.223 \pmod{451} \Rightarrow$
$d = 443 \Rightarrow c = 443$

Passo 4) Logo,

$$a \equiv b^r \pmod{n} \Rightarrow 443 \equiv 227^{106} \pmod{451}.$$

Algoritmo da Exponenciação

Outro algoritmo com a mesma finalidade do Algoritmo dos Quadrados Repetidos é o seguinte:

Entrada: inteiros a, e e n, sendo a, $n > 0$ e $e \geq 0$.
Saída: P tal que $a^e \equiv P \pmod{n}$, sendo P na forma reduzida ($0 \leq P < n$).

Etapa 1: Comece com $A = a$, $P = 1$ e $E = e$;
Etapa 2: Se $E = 0$ então $a^e \equiv P \pmod{n}$. Caso contrário, siga para a Etapa 3;

Etapa 3: Se E for ímpar, então atribua a P o valor do resto da divisão de AP por n e atribua a E o valor de $\frac{(E-1)}{2}$ e vá para a Etapa 5. Caso contrário, vá para a Etapa 4;
Etapa 4: Se E for par, então, atribua a E o valor $\frac{E}{2}$ e siga para a Etapa 5;
Etapa 5: Substitua o valor atual de A pelo resto da divisão de A^2 por n e volte para a Etapa 2.

Final: a forma reduzida de $a^e \pmod n$.

Exemplo.

Seja $a = 1521$, $e = 17$ e $n = 424$.
Etapa 1: $A = 1521$, $P = 1$ e $E = 17$.
Etapa 2: $E \neq 0$.
Etapa 3: E é ímpar. Façamos o resto da divisão de AP por n . Temos

$$1521 = (424.3) + 249 \Rightarrow P = 249$$

e

$$E = \frac{17-1}{2} = 8.$$

Etapa 5: $(1521)^2 = (424.5456) + 97 \Rightarrow A = 97$.

Etapa 2: $E \neq 0$.
Etapa 3: E é par. Passamos para Etapa 4.
Etapa 4: $E = \frac{8}{2} = 4$.
Etapa 5: $(97)^2 = (424.22) + 81$.
Logo, $A = 81$.

Etapa 2: $E \neq 0$.
Etapa 3: E é par. Passamos para Etapa 4.
Etapa 4: $E = \frac{4}{2} = 2$.
Etapa 5: $(81)^2 = (424.15) = 201$.
Logo, $A = 201$.

Etapa 2: $E \neq 0$.
Etapa 3: E é par. Passamos para Etapa 4.
Etapa 4: $E = \frac{2}{2} = 1$.
Etapa 5: $(201)^2 = (424.95) = 121$.
Logo, $A = 121$.

Etapa 2:$E \neq 0$.
Etapa 3: E é impar. Façamos o resto da divisão de AP por n. Temos

$$(121.249) = 30129 = (424.71) + 25 \Rightarrow P = 25$$

e

$$E = \frac{1-1}{2} = 0.$$

Etapa 5: $(121)^2 = (424.24) + 225 \Rightarrow A = 225$.

Etapa 2: $E = 0 \Longrightarrow 1521^2 \equiv 25 \bmod(424)$.

3 Criptografia RSA

3.1 Pré-Codificação

Para usarmos o método *RSA*, [1] e [4] , devemos converter uma mensagem em uma seqüência de números. Chamaremos essa etapa de *pré-ciframento.*
Para efeito de exemplificação, tomemos a seguinte tabela de conversão no pré-ciframento:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

s	t	u	v	w	x	y	z	_	0	1	2	3	4	5	6	7	8	9
28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46

Tabela 2

O espaço entre palavras será substituído pelo n^o. 36. Por exemplo, a frase "Famat 2007"[1], é convertida no número

$$15102210293639373744$$

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.
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 no pré-ciframento 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:

$$15 - 10 - 22 - 10 - 29 - 36 - 39 - 37 - 37 - 44.$$

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!).

3.2 Ciframento e Deciframento

Passemos ao processo de ciframento. Da subseção acima, temos $n = pq$ com p e q primos. Tomemos

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

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 ciframento.*
O par (n, e) é denominado *chave pública de ciframento do sistema RSA.*
Agora, cifremos cada bloco obtido no pré-ciframento (subseção anterior). Após o ciframento, os blocos não poderão ser reunidos de modo que não possamos distinguí-los, pois isto tornaria impossível o deciframento da mensagem.

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

O ciframento de um bloco b será denotado 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 $e = 701$ (observemos que $\text{mdc}(701, 1848) = 1$). Assim, o último bloco, 44, da mensagem anterior é cifrado como o resto da divisão de 44^{701} por 1943. Convertendo 701 em binário e utilizando o método dos quadrados repetidos, temos

$$1317 \equiv 44^{701} \pmod{1943}.$$

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

$$595 - 155 - 1849 - 155 - 841 - 384 - 1344 - 1168 - 1168 - 1317.$$

Para decifrar uma mensagem cifrada, 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 deciframento do sistema RSA.*
Seja $a = C(b)$ um bloco da mensagem cifrada, então $D(a)$ será o resultado do deciframento. 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, decifrando os blocos da mensagem cifrada, possamos encontrar a mensagem original, ou seja, $D(C(b)) = b$. O destinatário da mensagem não precisa, necessariamente, conhecer p e q para decifrá-la; basta conhecer n e d. É claro que para calcular d são necessários p e q, no entanto, o destinatário legítimo da mensagem não precisa conhecê-los.
No exemplo que estamos acompanhando, temos $n = 1943$ e $e = 701$.
Usando o Algoritmo Euclidiano Estendido, temos $d = 29$.
Assim, para decifrar o bloco 1317 recebido, devemos calcular o resto da divisão de 1317^{29} por 1943 (utilizando, por exemplo, o *Método dos Quadrados Repetidos*), ou seja, 44:

$$44 \equiv 1317^{29} \pmod{1943}.$$

Logo, a seqüência decifrada será

$$15 - 10 - 22 - 10 - 29 - 36 - 39 - 37 - 37 - 44,$$

que corresponde, via tabela de conversão, à frase "Famat 2007".

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 $q = 47$.

No ciframento:

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

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 o deciframento 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:

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

No deciframento:

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:

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

Deste modo, após encontrar o novo valor de d (positivo), então continua-se o deciframento usando o *Algoritmo dos Quadrados Repetidos*. Como $D(C(b)) = b$ e, para decifrar 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 neste deciframento, que é a mensagem inicial.

3.3 Demonstração da Funcionalidade do Sistema de Criptografia RSA

Precisamos verificar que se $C(b)$ é um inteiro e $1 \leq b < n$, então $D\left(C(b)\right) = b$. Na verdade, basta que $D\left(C(b)\right) \equiv b(\mathrm{mod}\, n)$, pois tanto $D\left(C(b)\right)$ quanto b estão no intervalo de 1 a $n-1$. Logo, b e $D\left(C\left(d\right)\right)$ só serão congruentes módulo n se forem iguais. Por isso, b deve ser menor que n e, mesmo depois de cifrados, os blocos devem se manter separados.
Por definição de D e C, temos:

$$D\left(C(b)\right) \equiv (b^e)^d \equiv b^{ed}(\mathrm{mod}\, n).$$

Como $n = pq$, vamos calcular $b^{ed}\left(\mathrm{mod}\, p\right)$ e $b^{ed}\left(\mathrm{mod}\, q\right)$. O cálculo para os dois módulos é análogo; logo, façamos apenas um deles.
Vejamos o caso de $b^{ed}\left(\mathrm{mod}\, p\right)$.
Como d é o inverso de $e\left(\mathrm{mod}\, \Phi\left(n\right)\right)$, temos

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

Daí,

$$b^{ed} \equiv b(b^{p-1})^{k(q-1)}(\mathrm{mod}\, p).$$

Usemos o *Pequeno Teorema de Fermat*, mas para isto, temos que supor que $p \nmid b$. Digamos que isto acontece, então

$$b^{p-1} \equiv 1(\mathrm{mod}\, p),$$

ou seja,

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

Analisando o caso em que $p \mid b$, temos que $b \equiv 0(\mathrm{mod}\, p)$. Logo, $b^{ed} \equiv b(\mathrm{mod}\, p)$ para qualquer valor de b.
Como $b^{ed} \equiv b(\mathrm{mod}\, p)$, analogamente, podemos mostrar que $b^{ed} \equiv b(\mathrm{mod}\, q)$. Daí, temos que $b^{ed} - b$ é divisível por p e q. Mas, como p e q são primos distintos, isto é, o $\mathrm{mdc}(p,q) = 1$, temos que $pq \mid \left(b^{ed} - b\right)$. Portanto, como $n = pq$, concluímos que $b^{ed} \equiv b(\mathrm{mod}\, n)$ para qualquer inteiro b.
Conclusão: $D\left(C\left(b\right)\right) = b$, como queríamos.

3.4 A Segurança do Sistema de Criptografia RSA

O método *RSA* é de chave pública, sendo p e q parâmetros do sistema e $n = pq$. A chave de criframento, o par (n, e), é a chave pública do sistema. Assim sendo, todos os usuários terão acesso a ela. Por isso, o *RSA* só será seguro se for difícil de encontrar d a partir de n e e.
Para encontrar d, utilizamos $\Phi(n)$ e e, mas para obtermos $\Phi(n)$, devemos ter p e q, que é a fatoração de n. Logo, para quebrar a cifra, devemos conseguir fatorar n, que é um problema extremamente difícil se n for grande.
Uma observação interessante é que, se acaso conhecermos $\Phi\left(n\right)$, saberemos quem são p e q. De fato:

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

Mas:

$$(p+q)^2 - 4n = (p^2 + q^2 + 2pq) - 4pq = (p-q)^2 \Rightarrow$$
$$p - q = \sqrt{(p+q)^2 - 4n} = \sqrt{(n - \Phi(n) + 1)^2 - 4n}$$

Tendo $p+q$ e $p-q$, obtemos p e q facilmente, tendo assim fatorado n.

Finalmente, a possibilidade de achar b, a partir de $C\left(b\right) \equiv b^e\left(\mathrm{mod}\, n\right)$ sem tentar achar d, é praticamente impossível se n é grande. Na verdade, acredita-se que quebrar o *RSA* e fatorar n são problemas equivalentes. No entanto, devemos tomar alguns cuidados, pois se p e q forem pequenos, se torna fácil encontrá-los. Ou se, mesmos grandes, $|p-q|$ for pequeno se torna fácil achá-los a partir de n, utilizando o *Algoritmo de Fermat*.

4 Assinaturas Digitais

Uma das aplicações da criptografia são as assinaturas digitais, que possuem um importante papel nas transações bancárias, obtendo assim uma maior segurança, tanto para o cliente, quanto para o banco.

Suponhamos que uma empresa realiza transações bancárias por computador. É óbvio que tanto a empresa quanto o banco queiram que a mensagem seja cifrada. Mas, como o *RSA* é um sistema de criptografia de chave pública, qualquer pessoa poderia enviar uma mensagem para fazer transações bancárias utilizando esse sistema. Por isso, é necessário que a mensagem esteja assinada eletronicamente.

Vejamos como mandar uma assinatura pelo *RSA*. Chamemos de C_e e D_e as funções de ciframento e deciframento da empresa e C_b e D_b as mesmas funções, só que do banco.

Sendo a um bloco de mensagem que a empresa vai enviar ao banco, o ciframento desse bloco seria $C_b(a)$. Para que a mensagem vá assinada, ela deve ser $C_b(D_e(a))$. Usamos primeiro a função deciframento da empresa ao bloco a e, depois, cifremos o bloco, usando a função ciframento do banco.

O banco, ao receber a mensagem $C_b(D_e(a))$, aplica a sua função de deciframento, obtendo $D_e(a)$, e, na seqüência, aplica a função ciframento da empresa, que é pública, para obter o bloco original a.

Somente a empresa conhece a função D_e. Portanto, se a mensagem fizer sentido, tem que ter tido origem na empresa, uma vez que a probabilidade de uma pessoa, sem conhecer D_e, mandar uma mensagem que faça sentido, após ser decifrada pelo banco, é praticamente nula. Assim, o banco pode estar seguro de que a mensagem é verdadeira.

5 Senhas Segmentadas

Suponhamos que para abrir o cofre de um determinado banco é necessário conhecer a senha que é um número s. Queremos partir a senha s entre n funcionários do banco. A cada funcionário do banco vai ser dado um elemento, alguns dígitos da senha s, que forma um conjunto S de n pares de inteiros positivos, de modo que, para um inteiro positivo $k \leq n$, previamente escolhido temos:

(i) qualquer subconjunto de S com k elementos permite determinar s.

(ii) é extremamente difícil determinar s conhecendo menos de k elementos de S.

Para construirmos o conjunto S, vamos ter utilizar o *Teorema do Resto Chinês*. Comecemos escolhendo um conjunto L de n inteiros positivos, dois a dois primos entre si. Determinemos N, o produto dos k menores números de L e M o produto dos $k-1$ maiores números de L. Definimos que este conjunto tem *limiar* k quando

$$N < s < M.$$

Observemos que esta condição implica que o produto de k ou mais elementos de é sempre maior que N e o produto de menos de k elementos é sempre menor que M. O conjunto S será formado pelos pares da forma (m, s_m) sendo $m \in L$ e s_m a forma reduzida de $s \pmod m$. O fato de termos um conjunto com limiar $k > 1$ implica que $s > m$, para qualquer $m \in L$.

Suponhamos que mais de k funcionários se encontram no banco. Isto é igual a dizer que são conhecidos t dentre os pares de S, onde $t \geq k$. Sejam esses pares (m_1, s_{m_1}), (m_2, s_{m_2}), (m_3, s_{m_3}), ..., (m_t, s_{m_t}). Vamos resolver o sistema de congruências:

$$\begin{cases} x \equiv s_{m_1} (\mathrm{mod}\, m_1) \\ x \equiv s_{m_2} (\mathrm{mod}\, m_2) \\ x \equiv s_{m_3} (\mathrm{mod}\, m_3) \\ \qquad \vdots \\ x \equiv s_{m_r} (\mathrm{mod}\, m_r) \end{cases}$$

obtendo x_0 como solução. De acordo com o *Teorema do Resto Chinês*,

$$x_0 = s(\mathrm{mod}\, m_1 m_2 \dots m_t).$$

Sabe-se que, como $t \geq k$,

$$m_1 m_2 \dots m_t \geq N > s.$$

Então, o sistema acima tem única solução menor que $m_1 m_2 \dots m_t$. Como s também é solução do sistema e $s < m_1 m_2 \dots m_t$, temos $s = x_0$.
Mas não é impossível resolver um sistema para o caso em que $t < k$. O problema é que o produto de menos de k módulos de L é sempre menor que s. Assim, a solução do sistema é congruente a s, mas não pode ser igual a s. Mas será possível encontrar s fazendo uma busca. De fato, sabemos que $M < s < N$ e que s satisfaz o sistema anterior, com $t < k$. Se acharmos uma das soluções x_0 do sistema, como $x_0 < M < s$, não encontramos s. Porém, o sistema será satisfeito por s, logo:

$$s = x_0 + y\,(m_1 m_2 \dots m_t)\,,$$

sendo y um inteiro positivo. Como:

$$N > s > M > x_0,$$

temos

$$\frac{M - x_0}{m_1 m_2 \dots m_t} \leq \frac{s - x_0}{m_1 m_2 \dots m_t} \leq \frac{N - x_0}{m_1 m_2 \dots m_t}.$$

Isto equivale a dizer que precisamos fazer uma busca para acharmos o valor correto de y entre, pelo menos,

$$d = \left[\frac{N - M}{m_1 m_2 \dots m_t}\right]$$

inteiros. Escolhendo os módulos de modo que d seja muito grande, fica praticamente impossível encontrar s por meio de uma busca. Porém, é sempre possível escolher um conjunto L satisfazendo a todas estas condições.
Na verdade os dados iniciais do problema são o número total de funcionários do banco e o número mínimo de funcionários que têm que estar presentes para que o cofre possa ser aberto, isto determina, respectivamente, a quantidade de elementos do conjnto L e o limiar k de L. Com estes dados, escolhemos um conjunto de L de limiar K. Com isto podemos calcular M e N como acima, escolhendo s de maneira aleatória no entervalo entre M e N. Deste modo, teremos todos os dados necessários para calcular S, que nos informa as senhas a serem distribuídas.
A segurança do sistema se baseia no valor de k. Quanto mais alto o valor de k, melhor. Significa que a senha será compartilhada por uma quantidade maior de funcionários do banco, o que torna mais seguro a segurança do sistema, pois teremos mais funcionários de prova para abrir o cofre do banco.

Vamos ver um exemplo disso: suponha que no banco existam 7 funcionários e que para se ter acesso ao cofre seja necessário, no mínimo, 2 desses funcionários. Logo, o conjunto L deve ter 7 elementos e o limiar deve ser 2. Fazendo uma escolha, usando apenas primos pequenos, deteminaremos uma possível escolha para L:

$$L = \{11, 13, 17, 19, 23, 29, 31\}\,.$$

O produto dos dois menores inteiros no conjunto é $N = 11.13 = 143$ e M é o produto dos $k-1$ maiores elementos de L. Como $k = 2$, temos que M é igual ao maior elemento de L, ou seja, $M = 31$.
O valor de s pode ser escolhido como sendo qualquer inteiro no intervalo que vai de 31 à 143. Digamos que $s = 42$. Então:

$$S = \{(11, 31)\,,\ \ (13, 29)\,, (19, 23)\,,\ \ (23, 19)\,, (29, 13)\,,\ \ (31, 11)\,,\ \ (37, 5)\}\,.$$

Imaginemos que os 2 funcionários que estejam no banco, cuja senha seja $(29, 13)$ e $(11, 31)$, queiram abrir o cofre. Para isto é necessário resolver o sistema:

$$\begin{cases} x \equiv 13 (\mathrm{mod}\, 29) \\ x \equiv 31 (\mathrm{mod}\, 11) \end{cases}.$$

A solução do sistema é $x = 42 + 319k$, sendo k um inteiro positivo. Isto é, $x \equiv 42 \,(\mathrm{mod}\, 319)$. Assim, determinamos s, que é o valor correto.

6 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 vice-versa. Mesmo em épocas recentes, como na Segunda Guerra Mundial, temos exemplos de cifras que foram quebradas, [7]. No entanto, a partir da década de 1970, com o surgimento da Criptografia *RSA* e dos diversos sistemas criptográficos dele derivados ou nele inspirados, os cifradores estão à frente dos quebradores de cifras.

Referências Bibliográficas

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

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

[6] 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.

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