Teoria dos Números e Criptografia

Prof. André L.B. Cavalcante, DSc

UPIS Faculdades Integradas – Faculdade de Tecnologia
Dept. Sistemas de Informação (andre02592@upis.br)

Resumo: O artigo apresenta de forma didática a integração entre as disciplinas teoria dos números e criptografia. Discorre sobre os objetivos e tipos de criptografia. Apresenta as cifras de substituição e de transposição para aplicação prática da criptografia simétrica. Como exemplo de criptografia assimétrica apresenta-se o algoritmo RSA. Também, são apresentados os algoritmos de Euclides e Fermat para fatoração de um número extenso e possível utilização na quebra da integridade do algoritmo RSA.

1. INTRODUÇÃO

Segundo Cavalcante (1997), Teoria dos números é uma ciência muito antiga, que visa primordialmente entender as propriedades e relações entre os números. Na busca de tais propriedades, surge uma grande interação entre este e vários outros ramos da matemática pura (como Álgebra, Análise Real e Complexa, Geometria) e aplicada (como Ciência da Computação e Criptografia).

A Criptografia é a ciência que estuda as formas de se escrever uma mensagem em código. Trata-se de um conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que apenas o destinatário a decifre e compreenda (Cavalcante, 2004).

Para tornar incompreensível a mensagem enviada define-se um protocolo aprovado pelo remetente e pelo destinatário, geralmente chamado de chave. A chave é base de qualquer criptografia, pois, é por meio dela que uma mensagem é codificada e decodificada.

A chave indica o nível de dificuldade para decodificar a mensagem. O fator de trabalho para decodificar uma mensagem encriptada é exponencial em relação ao tamanho da chave. Assim, pode-se dizer que uma chave com um tamanho de três dígitos gera mil possibilidades para o intruso lidar, e ao aumentar mais três dígitos a esta chave, ter-se-ia um milhão de possibilidades.

O tipo de chave usada depende do tipo da criptografia, isto é, simétrica ou assimétrica. A criptografia simétrica usa apenas uma chave privada (secreta) para encriptar e decriptar a mensagem, enquanto, a criptografia assimétrica usa um par de chaves. A primeira conhecida por chave pública, utilizada para encriptar a mensagem, e a segunda, por chave privada, utilizada pra decriptá-la.

Com a criptografia pretende-se garantir que uma mensagem só será lida e compreendida pelo destinatário autorizado, e para isso, é necessário que se cumpram quatro requisitos: confidencialidade, integridade, autenticação e não-recusa.

A confidencialidade obtida pela encriptação dos dados, assegura que só os receptores autorizados terão acesso às informações da mensagem.

A integridade assegura que a informação não será alterada durante o processo de transporte da informação. É obtida por meio da assinatura digital

Na autenticação, o remetente e o receptor podem confirmar as identidades uns dos outros assim como a origem e o destino da informação. É obtida por meio da assinatura digital e dos certificados.

Na não-recusa obtida por meio da assinatura digital e certificados, o remetente pode assiná-lo de forma digital, limitando legalmente a responsabilidade.

Infelizmente, para discutir os temas, assinatura digital e certificados, com mais cuidado seria necessário uma digressão muito longa, o que levaria longe demais das metas deste artigo, cujo escopo principal é apresentar algumas técnicas de encriptação, ou seja, de confidencialidade.

2. CRIPTOGRAFIA SIMÉTRICA

A criptografia simétrica foi o primeiro tipo de criptografia criado. Funciona transformando um texto em uma mensagem cifrada, por meio da definição de uma chave secreta, que será utilizada posteriormente para decriptar a mensagem, tornando novamente um texto simples (Cavalcante, 2004).

A criptografia simétrica utiliza apenas uma chave para codificar e decodificar uma mensagem. É usada em transmissões de dados em que não é necessário um grande nível de segurança como mensagens enviadas de um computador para outro, nas comunicações entre duas máquinas, no armazenamento da informação em um disco rígido.

A criptografia simétrica é relativamente rápida, contudo como desvantagem, não só o transmissor deve conhecer a chave como também o receptor. Além disso, o volume total dos dados transmitidos é limitado pelo tamanho da chave.

2.1 Métodos de Criptografia Simétrica

Os métodos de criptografia simétrica têm sido divididos em duas categorias: as cifras de substituição e as de transposição.

2.1.1 Cifras de Substituição

Cada grupo de letras é substituído por outro grupo de letras. A Tabela 1 apresenta um exemplo bem simples, só para entendimento da idéia. Cada uma das 26 letras do alfabeto tem um correspondente em outra letra.

Tabela 1: Cifras de substituição

a	b	c	d	e	f	g	h	i	j	k	l	m
Q	W	E	R	T	Y	U	I	O	P	A	S	D
n	o	p	q	r	s	t	u	v	x	y	z	w
F	G	H	J	K	L	Z	X	C	V	B	N	M

Esse sistema é conhecido como cifras de substituição. Substituindo as letras da palavra "paixão" pela correspondente resultaria em "HQOVQG".

Em um texto pequeno, a cifra pode ser descoberta facilmente, pois o intruso pode proceder da seguinte forma:

- Contar as letras mais frequentes do texto cifrado.
- Atribuir a letra "a" a cifra que mais aparece no texto cifrado.
- Verificar os trigamas e encontrar um no formato gXi, o que sugere que X seja "u".

2.1.2 Cifras de Transposição

As cifras de transposição utilizam o princípio de mudança da ordem das letras da mensagem a ser enviada. Inicialmente, escolhe-se uma palavra para representar a chave. Por exemplo, considere a chave sendo a palavra "brasil", e a mensagem o texto "minha linda, onde te encontro?".

A chave serve de apoio para enumerar as colunas na ordem alfabética crescente das letras (Tabela 2). A mensagem é escrita abaixo da chave, de 6 em 6 letras (que neste caso, é a mesma quantidade de letras da chave).

Tabela 2: Cifra de transposição

b	r	a	s	i	l
2	5	1	6	3	4
m	i	n	h	a	l
i	n	d	a	o	n
d	e	t	e	e	n
c	o	n	t	r	o

O texto é lido na vertical, conforme a ordem das colunas, resultando em:

"ndtnmidcaoerlnnoineohaet".

Em alguns algoritmos, utiliza-se uma combinação entre as cifras de substituição e as de transposição, dificultando um pouco mais a decodificação da mensagem. Também é possível, utilizar algum símbolo que represente os espaços entre as palavras da mensagem.

2.1.3 Matriz

Embora a criptografia moderna utilize as mesma idéias básicas da substituição e transposição, a ênfase atual é diferente, e tem como objetivo tornar o algoritmo complexo, para que o intruso não seja capaz de obter qualquer sentido da mensagem.

Desta forma, uma outra maneira de codificar uma mensagem utilizando o conceito da criptografia simétrica é por meio de multiplicação da matriz mensagem por outra matriz chave. Um exemplo dessa codificação pode ser dado pela associação das letras do alfabeto aos números, segundo a correspondência da Tabela 3.

Tabela 3: Cifras matriz

a	b	c	d	e	f	g	h	i
1	2	3	4	5	6	7	8	9
j	k	l	m	n	o	p	q	r
10	11	12	13	14	15	16	17	18
s	t	u	v	x	y	z	w	-
19	20	21	22	23	24	25	26	0

Suponha que a mensagem a ser criptografada seja “EU TE AMO”. Pode-se formar uma matriz 3 x 3, que usando a correspondência numérica da cifra matriz torna-se:

$$\begin{bmatrix} E & U & - \\ T & E & - \\ A & M & O \end{bmatrix} = \begin{bmatrix} 5 & 21 & 0 \\ 20 & 5 & 0 \\ 1 & 13 & 15 \end{bmatrix} \quad (1)$$

Suponha também que a chave para esta codificação seja a palavra "PACIÊNCIA". Seja *C* uma matriz qualquer 3 x 3 inversível, que descreve esta chave*:*

$$\begin{bmatrix} P & A & C \\ I & E & N \\ C & I & A \end{bmatrix} = \begin{bmatrix} 16 & 1 & 3 \\ 9 & 5 & 14 \\ 3 & 9 & 1 \end{bmatrix} \quad (2)$$

Multiplica-se a matriz mensagem por *C*, obtendo-se *MC*.

$$\begin{bmatrix} 5 & 21 & 0 \\ 20 & 5 & 0 \\ 1 & 13 & 15 \end{bmatrix} \begin{bmatrix} 16 & 1 & 3 \\ 9 & 5 & 14 \\ 3 & 9 & 1 \end{bmatrix} = \begin{bmatrix} 269 & 110 & 309 \\ 365 & 45 & 130 \\ 178 & 201 & 200 \end{bmatrix} \quad (3)$$

Transmite-se esta nova matriz (na prática, envia-se a cadeia de números 269, 110, 309, 365, 45, 130, 178, 201, 200).

Quem recebe a mensagem decodifica-a por meio da multiplicação pela inversa ($(M \bullet C) \bullet C^{-1} = M$) e posterior transcrição dos números para letras. *C* é chamada *matriz chave* para o código.

A matriz C^{-1} é obtida resolvendo-se a equação matricial $C.C^{-1} = I_3$, onde I_3 é a matriz identidade de ordem 3:

$$\begin{bmatrix} 16 & 1 & 3 \\ 9 & 5 & 14 \\ 3 & 9 & 1 \end{bmatrix} \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (4)$$

3. DISTRIBUIÇÃO DOS NÚMEROS PRIMOS

Diz-se que um inteiro positivo $p > 1$ é um número primo se e somente se 1 e *p* são os únicos divisores positivos. Em outros termos, um inteiro positivo $p > 1$ é um primo se e somente se *p* não possui um divisor *d* tal que $1 < d < p$. Um inteiro positivo $a > 1$ que não é primo diz-se um *número composto* (Hardy & Wright, 1960 e Cavalcante, 1997).

Observa-se que por estas definições, o inteiro positivo 1 não é primo nem composto, e por conseguinte se *a* é um inteiro positivo qualquer, então *a* é primo, ou *a* é composto, ou $a = 1$. A Tabela 4 apresenta a lista dos cem primeiros números primos.

Denota-se, ainda, por $\pi(x)$ o número de números primos positivos que não excedem *x* (Hardy & Wright, 1960 e Cavalcante, 1997).

Teorema 1: O número de números primos é infinito, isto é, se $x \to \infty$ então $\pi(x) \to \infty$.

Demonstração:

Sejam 2, 3, ..., *p* todos os números primos que não excedem *p* e seja $q = 2.3....p + 1$. Então *q* não é múltiplo de 2, 3, ..., *p*. Desta forma, ou *q* é primo ou *q* é divisível por um primo entre *p* e *q*. Portanto sempre existe um primo maior do que *p*. Daí segue que o número de primos é infinito.

A distribuição dos números primos é um dos mais interessantes ramos da Teoria dos Números. Vários teoremas e conjecturas encontrados são principalmente resultados de observações empíricas. Por exemplo, a partir da Tabela 5 (Cavalcante, 1997) pode-se conjecturar:

- Existem relativamente "poucos" primos, quando comparados com todos os inteiros.
- $\pi(x) \to x/\log(x)$ quando $x \to \infty$.

Tabela 4: Lista de primos

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541

Tabela 5: Distribuição dos primos

x	π(x)	x/log(x)
1000	168	145
10000	1229	1086
50000	5133	4621
100000	9592	8686
500000	41538	38103
1000000	78498	72382
2000000	148933	137848
5000000	348513	324149
10000000	664579	620417
20000000	1270607	1189676
90000000	5216954	4913897
100000000	5761455	5428613
1000000000	50847534	48254630

A Figura 1 apresenta a comparação das funções π(x) e x/log(x). A distribuição dos números primos é uma análise que já tem sido feita a muito tempo. De fato, estes resultados foram demonstrados e podem ser encontrados em Hardy & Wright (1960), Keng (1982) e Cavalcante (1997).

4. CONGRUÊNCIAS

Sejam $a, b, m \in N$. Se $a - b$ for um múltiplo de *m* diz-se que *a* e *b* são *congruentes módulo m*, e escreve-se $a \equiv b \pmod{m}$ (Keng, 1982 e Cavalcante, 1997).

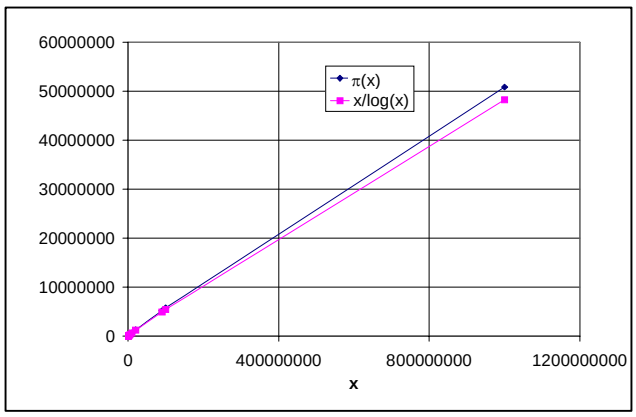

Figura 1: Comparação entre π(x) e x/log(x).

Teorema 2: (Propriedades Fundamentais da Congruência) Para quaisquer *a*, *b* e *c* ∈ *Z*, tem-se que:

(i) $a \equiv a \pmod{m}$.

(ii) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

(iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Demonstração:

Sejam *t*, *k*, *m* ∈ *Z*,

(i) *a* - *a* = 0 = *tm*, para *t* = 0. Logo, $a \equiv a \pmod{m}$.

(ii) Se $a \equiv b \pmod{m}$, então *a* - *b* = *tm*. Por outro lado, *b* - *a* = (-*t*)*m* e, portanto, $b \equiv a \pmod{m}$.

(iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então *a* - *b* = *tm* e *b* - *c* = *km*. Da segunda, tem-se que *b* = *c* + *km*. Portanto, da primeira tem-se, *a* - (*c* + *km*) = *tm*, ou seja, *a* - *c* = (*t* + *k*)*m*, logo $a \equiv c \pmod{m}$.

5. ALGORITMO DE EUCLIDES

O algoritmo de Euclides foi descrito nas proposições 1 e 2 do Livro 7 dos Elementos, mas acredita-se que a origem do mesmo seja muito anterior.

Sejam *a* e *b* inteiros positivos e $a \geq b$. Deseja-se calcular o máximo divisor comum entre *a* e *b*, isto é, MDC(*a*, *b*) (Keng, 1982 e Cavalcante, 1997). Para utilização do algoritmo deve-se proceder da seguinte forma:

- O algoritmo euclidiano consiste em dividir *a* por *b*, achando o resto r_1. Se $r_1 \neq 0$, divide-se *b* por r_1, obtendo o resto r_2.
- Se $r_2 \neq 0$, divide-se r_1 por r_2, obtendo o resto r_3.
- E assim por diante. O último resto diferente de zero desta seqüência de divisões é o máximo divisor comum entre *a* e *b*.

Exemplos da utilização deste algoritmo são apresentados nos itens 6 e 7.

6. CRIPTOGRAFIA ASSIMÉTRICA

A criptografia assimétrica, também conhecida como de chave pública, utiliza duas chaves: uma pública, que todos conhecem, e outra privada. A primeira para cifrar o texto ou mensagem, e a segunda para decifrar (Cavalcante, 2004).

A criptografia assimétrica pode ser empregada para assinatura digital e autenticação. Neste caso, é criada uma chave privada e a partir dela uma chave pública que deve ser enviada para todas as pessoas com as quais se deseja trocar informações. Um dos algoritmos mais famosos é o RSA.

6.1 Algoritmo RSA

O algoritmo RSA leva a inicial do nome dos criadores Ron Revista, Adi Shamir e Len Adleman. O RSA utiliza duas chaves criptográficas, uma chave pública e uma privada. A chave pública é usada para criptografar a mensagem, enquanto a chave privada, para decriptografá-la (Buchmann, 2002).

A segurança desse método se baseia na dificuldade de fatorar números extensos. Segundo pesquisadores, a fatoração de um número de 200 dígitos requer 4 milhões de anos para ser processada. Fatorar um número de 500 dígitos exige 10^{25} anos. Mesmo que os computadores se tornem mais velozes, muito tempo irá passar até que seja possível fatorar um número de 500 dígitos, e até lá poderão escolher a fatoração de um número ainda maior.

Para utilização do método deve-se proceder com as seguintes etapas:

- São escolhidos dois números primos extensos *p* e *q* (geralmente maiores que 10^{100}).
- Calcula-se:

$$n = pq \tag{5}$$

$$\phi(n) = (p-1)(q-1) \tag{6}$$

- Escolhe-se um número *d* que seja co-primo a $\phi(n)$, isto é, MDC(*d*, $\phi(n)$) = 1.
- Encontra-se *e* de forma que:

$$e \cdot d \equiv 1 \pmod{\phi(n)} \tag{7}$$

- O texto simples é dividido em blocos, de modo que cada mensagem, *M*, fique no intervalo $0 \leq M < n$.

- Para criptografar a mensagem, *M*, é calculado:

$$C \equiv M^{e} \pmod{n} \quad (8)$$

- Para decriptografar *C*, é calculado:

$$M \equiv C^{d} \pmod{n} \quad (9)$$

É possível provar que, para todo *M* na faixa especificada, as funções de criptografia e decriptografia são inversas entre si. Para realizar a criptografia, é necessário conhecer o valor do "*e*" e do "*n*", ao passo que para decriptografar, são necessários "*d*" e "*n*". Portanto, a chave pública consiste no par (*e*, *n*) e a chave privada consiste em (*d*, *n*).

Exemplo 1: Utilize o algoritmo RSA para encriptar a palavra ANDRÉ, utilize as cifras matriz (Tabela 3).

Escolhe-se $p = 3$ e $q = 11$.
Calcula-se : $n = p.q = 3.11 = 33$
$\phi(n) = (p - 1)(q - 1) = (3 - 1)(11 - 1) = 20$

O valor escolhido como número *d* que seja co-primo a $\phi(n)$ deve satisfazer a equação MDC(20, d) = 1. Desse modo, pelo algoritmo de Euclides, d = 7.

	2	1	6
20	7	6	1
6	1	0	

Portanto, a chave privada consiste em (*d*, *n*) = (7, 33).

Para que a equação $e.d \equiv 1 \pmod{\phi(n)}$ seja verdadeira o "*e*" deverá ser um número que multiplicado por 7 (mod 20) seja igual a 1. Usando o método da tentativa e erro, 1 não daria certo, pois 1.7 (mod 20) ≠ 1. 2 também não daria certo, pois 2.7 (mod 20) ≠ 1. O número 3 se identifica, pois 3.7 (mod 20) = 1, portanto, a chave pública consiste em (*e*, *n*) = (3, 33).

Representando cada letra do alfabeto por um número, conforme a Tabela 3 (cifras matriz), chega-se a Tabela 6:

Tabela 6: Criptografia

Simbólico	Numérico	M^3	$C=M^3 \pmod{33}$
A	1	1	1
N	14	2744	5
D	4	64	31
R	18	5832	24
E	5	125	26

A Tabela 7 apresenta o processo de decriptar a mensagem.

Tabela 7: Decriptografia

$C=M^3 \pmod{33}$	C^7	$M=C^7 \pmod{33}$	Simbólico
1	1	1	A
5	78125	14	N
31	31^7	4	D
24	24^7	18	R
26	26^7	5	E

7. FUNÇÃO MAIOR INTEIRO

Chama-se parte inteira de um número real *x* o inteiro *n* que verifica à condição: $n \le x < n + 1$. Em outros termos, parte inteira de um número real *x* é o maior inteiro *n* que não excede *x* (Keng, 1982 e Cavalcante, 1997).

A parte inteira de um número real *x* indica-se pelo símbolo [*x*], que se lê: "parte inteira de *x*". Portanto, subsistem as desigualdades:

$$[x] \le x < [x] + 1 \Rightarrow x - 1 < [x] \le x \quad (10)$$

Note-se que [*x*] = *x* se e somente se *x* é um inteiro, e que todo número real *x* pode escrever-se sob a forma:

$$x = [x] + k, \text{ onde } 0 \le k < 1 \quad (11)$$

Além disso, obviamente:

$$\sum_{1 \le n \le x} 1 = [x] \quad (12)$$

A função $f : R \to Z$ definida por f(*x*) = [*x*] chama-se função maior inteiro.

8. ALGORITMO DE FERMAT

Se fosse possível fatorar o valor de *n* (publicamente conhecido), seria possível então encontrar *d* utilizando-se o algoritmo de Euclides, porém fatorar números extensos é extremamente difícil. Nesta seção apresenta-se o algoritmo de Fermat, utilizado para fatorar números, e algumas aplicações (Coutinho, 2003).

O algoritmo de Fermat recebe um inteiro positivo ímpar *n* e retorna um fator de *n* ou uma mensagem indicando que *n* é primo. Consiste das seguintes etapas:

- Etapa 1: Comece com $x = \lceil \sqrt{n} \rceil$; se $n = x^2$ então *x* é fator de *n* e pode-se parar.
- Etapa 2: Caso contrário incremente *x* de uma unidade e calcule $y = \sqrt{x^2 - n}$.
- Etapa 3: Repita a etapa 2 até encontrar um valor inteiro para *y*, ou até que *x* seja igual a (*n* + 1)/2:

no primeiro caso n tem fatores $x + y$ e $x – y$, no segundo n é primo.

Exemplo 2: Ao utilizar um algoritmo RSA, adotou-se n = 116617, descubra o valor da chave privada (d, n).

Seja n = 116617 o número que se quer fatorar. A variável x é inicializada com a parte inteira da raiz quadrada de n, que neste caso vale x = 341. Mas

$$x^2 = 341^2 = 116281 < 116617,$$

logo passa-se a incrementar x de um em um. Faz-se isto até que $\sqrt{x^2 - n}$ seja inteiro, ou x seja igual a (n + 1)/2, que neste caso vale 58309. É mais fácil resumir isto em uma Tabela 8.

Tabela 8: Resultado do algoritmo de Fermat

x	y
342	18,63
343	32,12
344	41,46
345	49,07
346	55,67
347	61,58
348	66,99
349	72,00

Obteve-se assim um inteiro no oitavo laço. Portanto, x = 349 e y = 72 são os valores desejados. Os fatores correspondentes são $x + y$ = 421 e $x – y$ = 277. Deste fato, tem-se:

$$\phi(n) = (421 - 1)(277 - 1) = 115920,$$

e, além disso, $mdc(\phi(n), d) = 1$. Utilizando o algoritmo de Euclides, é fácil perceber que para d = 11, esta equação é verificada.

	10538	5	2
115920	11	2	1
2	1	0	

E, portanto, a chave privada (d, n) = (11, 116617).

Exemplo 3: Ao utilizar um algoritmo RSA, adotou-se n = 250517, descubra o valor da chave privada (d, n).

Seja n = 250517 o número que se quer fatorar. A variável x é inicializada com a parte inteira da raiz quadrada de n, que neste caso vale x = 500. Mas

$$x^2 = 500^2 = 250000 < 250517,$$

logo passa-se a incrementar x de um em um. Faz-se isto até que $\sqrt{x^2 - n}$ seja inteiro, ou x seja igual a (n + 1)/2, que neste caso vale 125259. Neste caso, com apenas um laço, tem-se que x = 501 e y = 22 são os valores desejados. Os fatores correspondentes são $x + y$ = 523 e $x – y$ = 479. Deste fato, tem-se:

$$\phi(n) = (523 - 1)(479 - 1) = 249516,$$

e, além disso, $mdc(\phi(n), d) = 1$. Utilizando o algoritmo de Euclides, é fácil perceber que para d = 5, esta equação é verificada.

	49903	5
249516	5	1
1	0	

E, portanto, a chave privada (d, n) = (5, 250517).

Exemplo 4: Ao utilizar um algoritmo RSA, adotou-se n = 9981401593 (extenso), descubra o valor da chave privada (d, n).

Seja n = 9981401593 o número que se quer fatorar. A variável x é inicializada com a parte inteira da raiz quadrada de n, que neste caso vale x = 99906. Mas

$$x^2 = 99906^2 = 9981208836 < 9981401593,$$

logo passa-se a incrementar x de um em um. Faz-se isto até que $\sqrt{x^2 - n}$ seja inteiro, ou x seja igual a (n + 1)/2, que neste caso vale 4990700797. Neste caso, com apenas um laço, tem-se que x = 99907 e y = 84 são os valores desejados. Os fatores correspondentes são $x + y$ = 99991 e $x – y$ = 99823. Deste fato, tem-se:

$$\phi(n) = (99991 - 1)(99823 - 1) = 9981201780,$$

e, além disso, $mdc(\phi(n), d) = 1$. Utilizando o algoritmo de Euclides, é fácil perceber que para d = 7, esta equação é verificada.

	1425885968	1	1	3
9981201780	7	4	3	1
4	3	1	0	

E, portanto, a chave privada (d,n)=(5, 9981401593).

Exemplo 5: Ao utilizar um algoritmo RSA, adotou-se n = 249863005313 (extenso), descubra o valor da chave privada (d, n).

Seja n = 249863005313 o número que se quer fatorar. A variável x é inicializada com a parte inteira da raiz quadrada de n, que neste caso vale x = 499862. Mas

$$x^2 = 249862019044 < n,$$

logo passa-se a incrementar x de um em um. Faz-se isto até que $\sqrt{x^2 - n}$ seja inteiro, ou x seja igual a $(n + 1)/2$, que neste caso vale 124931502657. Neste caso, com apenas um laço, tem-se que x = 499863 e y = 116 são os valores desejados. Os fatores correspondentes são $x + y$ = 499979 e $x - y$ = 499747. Deste fato, tem-se:

$$\phi(n) = (499979 - 1)(499747 - 1) = 249862005588,$$

e, além disso, $mdc(\phi(n), d) = 1$. Utilizando o algoritmo de Euclides, é fácil perceber que para d = 5, esta equação é verificada.

	49972401117	1	1	2
249862005588	5	3	2	1
3	2	1	0	

E, portanto, a chave privada (d, n) = (5, 249863005313).

9. CONCLUSÕES E SUGESTÕES

A criptografia assimétrica é mais segura que a simétrica, por não precisar comunicar o receptor a chave necessária para decriptografar a mensagem e, pode ser utilizada em assinatura digital. No entanto, a principal desvantagem consiste no fato de a criptografia assimétrica ser mais lenta do que a simétrica.

O algoritmo de Fermat utilizado para fatoração de números extensos, apesar de bem interessante, na maioria dos casos leva a um processo de muitos laços, inviabilizando a quebra da integridade do modelo RSA. O que faz o modelo RSA ainda ser uma excelente escolha para criptografar mensagens, pois não existe um critério tão eficiente de fatoração.

De maneira a tornar não possível a fatoração do n do modelo RSA, é necessário escolher adequadamente os fatores primos p e q. Na hora da escolha destes números primos é necessário um determinado *feeling*, pois como observado nos exemplos 4 e 5, não basta apenas que os números primos sejam extensos, é necessário também, que os mesmos não estejam próximos.

Como sugestão para pesquisas futuras, seria interessante combinar a criptografia simétrica com a assimétrica, somando a segurança com a rapidez. Além disso, sugere-se também a necessidade de continuar o estudo sobre a distribuição dos números primos, para melhor entendimento do limite mínimo de afastamento entre os números primos escolhidos no modelo RSA.

10. REFERÊNCIAS BIBLIOGRÁFICAS

Buchmann, J.A. Introdução à Criptografia. São Paulo: Berkeley (2002).

Cavalcante, A.L.B. Tópicos em Teoria dos Números. Relatório PIBIC/CNPq. Universidade de Brasília (1997).

Cavalcante, A.L.B. Matemática II. Notas de Aula. Brasília: Editora UPIS (2004).

Coutinho, S.C. Números Inteiros e Criptografia RSA. Rio de Janeiro: IMPA. Série de Computação e Matemática (2003).

Hardy, G.H. & Wright, E.M. An Introduction to the Theory of Numbers. 4th ed. Oxford (1960).

Keng, H.L. Introduction to Number Theory. Springer-Verlag (1982).