

## UMA INTRODUÇÃO A CRIPTOGRAFIA RSA. Elen Viviani Pereira da Silva, Jaime Edmundo Apaza Rodriguez.-1.01- Matemática - Departamento de Matemática - Faculdade de Engenharia de Ilha Solteira - Campus de Ilha Solteira.

Durante milhares de anos, reis e rainhas dependiam de algum tipo de comunicação para governar seus países. Ao mesmo tempo, todos estavam cientes dos riscos das mensagens serem interceptadas pelo inimigo. Foi essa ameaça que gerou o desenvolvimento de métodos para mascarar as mensagens, denominados códigos e cifras.

A proliferação dos computadores e sistemas de comunicação, em 1960, criou uma grande demanda do setor privado buscando, na Criptografia, meios para proteger a informação na forma digital e fornecer serviços de segurança. Um trabalho relevante na pesquisa sobre Criptografia apareceu em 1976, quando *W. Diffie* e *M. Hellman* publicaram o artigo *New Directions in Cryptography*. Este trabalho introduz o conceito inovador de *Criptografia de Chave Pública*, ou assimétrica, e fornece um novo e engenhoso método para a troca de chave.

Neste trabalho abordamos o *método Criptográfico RSA*, que trabalha com algoritmos computacionais utilizando a chave pública. Esse código foi inventado em 1978 por *R. L. Rivest*, *A. Shamir* e *I. Adleman*, que na época trabalhavam no Massachusetts Institute of Technology (M.I.T). Atualmente, o RSA é o método mais usado em aplicações comerciais. Um dos exemplos de sua aplicação está no Netscape, o mais popular dos softwares de navegação na internet.

Para a descrição e implementação do método RSA, usamos resultados da teoria dos números, assim como técnicas para implementação de algoritmos de fatoração de números inteiros. O método trabalha fundamentalmente com propriedades do anel  $Z_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$  e com o grupo cíclico  $U(n) = \{\overline{a} \in Z_n \mid \text{mdc}(a, n) = 1\}$ . Alguns resultados e propriedades usadas são as seguintes:

**Pequeno Teorema de Fermat.** Sejam,  $p$  um número primo e  $a$  um número inteiro. Então  $a^{p-1} \equiv 1 \pmod{p}$ .

**Teorema de Euler.** Sejam  $n$  e  $a$  números inteiros tais que  $\text{mdc}(a, n) = 1$ , então  $a^{\phi(n)} \equiv 1 \pmod{n}$ .

**A função de Euler ( $\phi$ ).** Se  $m, n$  são inteiros positivos tais que  $\text{mdc}(m, n) = 1$ , então  $\phi(mn) = \phi(m)\phi(n)$ .

**Teorema de Wilson.** Se  $p$  é um inteiro positivo tal que  $(p-1)! \equiv -1 \pmod{p}$ , então  $p$  é primo.

**Teorema de Lagrange.** Em um grupo finito, a ordem de qualquer subgrupo divide a ordem do grupo.

**Teorema da Raiz Primitiva.** Se  $p$  é um número primo, então o grupo  $U(p)$  é cíclico.

**Teste de Lucas.** Seja  $n$  um inteiro positivo ímpar e  $b$  um inteiro tal que  $2 \leq b \leq n-1$ . Se  $b^{n-1} \equiv 1 \pmod{n}$  e  $b^{(n-1)/p} \not\equiv 1 \pmod{n}$ , para cada fator primo  $p$  de  $n-1$ , então  $n$  é primo.

A chave de codificação do RSA é essencialmente constituída por  $n = pq$ , onde  $p$  e  $q$  são primos grandes. A precodificação inicia-se com a escolha de  $p, q$  e um inteiro  $e$  de forma que  $\text{mdc}(e, \phi(n)) = 1$ . O par  $(n, e)$  é feito público. Cada letra do alfabeto é colocada em correspondência biunívoca com um número de dois algarismos. Analogamente, ao espaço entre as palavras deve corresponder um número, também de dois algarismos e diferente dos demais. Após transformar a mensagem, é obtida uma seqüência de números, a qual é preciso separar em blocos de modo que cada bloco,  $M$ , satisfaça a condição  $M^{\phi(n)} \equiv 1 \pmod{n}$  (*Teorema de Euler* para  $M$  e  $n$ ).

Denotaremos o bloco por  $M_i$ , onde  $i = 1, 2, \dots, k$ . A codificação é feita de forma que cada bloco codificado seja o resto da divisão de  $M_i^e$  por  $n$ , ou seja, devemos calcular  $C(M)$  de forma que  $M_i^e \equiv C(M) \pmod{n}$ .

O processo de decodificação é feito através da determinação de um número inteiro positivo  $d$  tal que  $ed \equiv 1 \pmod{\phi(n)}$ . Essa congruência é facilmente calculada pelo *Algoritmo Euclidiano Estendido*.

Mostraremos um exemplo. Vamos codificar a mensagem “*Cifrar é uma arte*”. Primeiramente, com ajuda da tabela abaixo, fazemos a pre-codificação.

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	Y	X	Z	—									
28	29	30	31	32	33	34	35	99									

Obtemos assim a sequência:

1218152710279914993022109910272914.

Escolhemos  $n = 11 \cdot 7 = 77$  e  $e = 11$ . Calculando a ordem de  $n$ , através da propriedade da *função de Euler*, obtemos  $\phi(77) = \phi(11)\phi(7) = 10 \cdot 6 = 60$ . Neste caso, a mensagem pode ser quebrada nos seguintes blocos:

121 – 81 – 527 – 102 – 79 – 914 – 99 – 302 – 210 – 99 – 102 – 72 – 914.

A seguir, cada bloco é codificado. Por exemplo, codificando o bloco 121 da mensagem, obtemos

$$121^{11} \equiv 44^{11} \equiv (121)^3 11 \equiv (44)^3 11 \equiv 11 \pmod{77}.$$

Assim  $C(121) = 11$ . Repetindo o processo para todos os blocos obtemos a mensagem cifrada abaixo:

11373258462322715622583923.

Para decifrar a mensagem, temos que determinar  $d$ , resolvendo a equação diofantina  $11d + y60 = 1$ . Neste caso, obtemos  $d = 11$ . Tomando o bloco 121 acima, basta decodificar:

$$11^{11} \equiv (44)^5 11 \equiv (44)^2 11 \equiv 121 \pmod{77}.$$

Obtemos assim a sequência inicial, e portanto, recuperamos a mensagem.

Como já se sabe, o RSA é um método de chave pública, pois o par  $(n, e)$  é acessível a qualquer usuário. Na prática, só podemos achar  $d$  se soubermos a ordem  $\phi(n)$  e  $e$ . Desta forma, é preciso fatorar  $n$ , e se este for muito grande, isto se torna um problema muito complexo. Existem muitos algoritmos (probabilísticos) de fatoração de números inteiros, eficientes em alguns casos, mas ainda estudam-se métodos determinísticos de fatoração em tempo não exponencial, pois fatorar um número inteiro composto  $n$ , muito grande, implica tempo e custos computacionais altos. Assim, podemos concluir que o método oferece um alto grau de segurança e bom desempenho.

O método de Criptografia RSA constitui um exemplo de aplicação de vários ramos da matemática na solução do problema da transmissão de informação com segurança em tempo real. Este método garante a transmissão de informações confidenciais através de redes inseguras, tornando-se assim de extrema importância na atualidade.

Referências:

- [1] Coutinho, S. C., *Primalidade em Tempo Polinomial- Uma Introdução ao Algoritmo AKS*, Coleção Iniciação Científica, Sociedade Brasileira de Matemática, 2004.
- [2] Coutinho, S. C., *Números Inteiros e Criptografia*, Série de Computação e Matemática, IMPA, Segunda Edição, 2003.
- [3] Lenstra, A., Tromer, E., Shamir, A., Kortsmit, W., Dodson B., Hughes J. and Leyland, P., *Factoring Estimates para a 1024-bit RSA modulus*, Asiacrypt 2003.
- [4] Lenstra, A., *Computational Methods in Public Key Cryptology*, Institute for Mathematical Sciences, National University of Singapore, 2002.
- [5] Menezes, A., Oorschot, P.V., Vanstone, S., *Handbook of Applied Cryptography*, CRC, Press, 1996.
- [6] Rivest, R. L., Shamir, A., Adleman, L., *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications, Programming Techniques SL Graham, RL Rivest Editors, 1978.

**Bolsa:** FAPESP