

Robinson Alves Lemos

Introdução à Criptografia RSA

Barra do Bugres

2009

Sumário

1	Criptografia RSA	2
1.1	Pré-Codificação	2
1.1.1	Conversão: Mensagem para Código	2
1.1.2	Escolher Parâmetros	2
1.1.3	Quebrar o Número	3
1.2	Codificação	3
1.2.1	Chave de Codificação	3
1.2.2	Codificando um Bloco	3
1.3	Decodificação	4
1.3.1	Chave de Decodificação	4
1.3.2	Decodificando um Bloco	4
	Referências	5

1 *Criptografia RSA*

O mais conhecido dos métodos de criptografia de chave pública é o RSA. Este código foi inventado em 1978 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachusetts Institute of Technology (M.I.T.). As letras RSA correspondem às iniciais dos inventores do código. Há vários outros códigos de chave pública, mas o RSA é, atualmente, o mais usado em aplicações comerciais. (COUTINHO, 1997)

1.1 Pré-Codificação

1.1.1 Conversão: Mensagem para Código

No primeiro passo convertemos a mensagem em um número utilizando, por exemplo, a seguinte tabela:

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	21	22	23	24
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
25	26	27	28	29	31	32	33	34	35	36	37	38

Para espaço em branco utilizaremos o número 99.

Exemplo 1.1. A mensagem: *Mensagem Secreta* ficaria convertida na seguinte forma:

241525311111715249931151329153211

1.1.2 Escolher Parâmetros

O segundo passo da Pré-codificação é a escolha dos parâmetros:

Dois números primos: p e q ;

O produto dos dois números primos: $n = pq$.

Exemplo 1.2. $p = 17$, $q = 23$ e $n = 17 \cdot 23 = 391$.

1.1.3 Quebrar o Número

O último passo da Pré-Codificação é quebrar o longo número obtido na conversão em blocos de números. Cada bloco será um número menor que n .

Exemplo 1.3. Em nosso exemplo, $n = 391$ e, assim,

Número obtido na conversão:

24152531111715249931151329153211

Número separado em blocos:

241 – 52 – 53 – 111 – 171 – 52 – 49 – 93 – 115 – 132 – 91 – 53 – 211

1.2 Codificação

1.2.1 Chave de Codificação

A chave de codificação é dada por um par de números: (n, c) , onde n é o produto dos dois primos p e q e c é um inteiro positivo inversível módulo $\phi(n)$ (isto é, $\text{mdc}(\phi(n), c) = 1$).

1.2.2 Codificando um Bloco

Se x é um bloco não codificado e $C(x)$ é o bloco codificado, então:

$C(b)$ é o resto da divisão de x^c por n .

Exemplo 1.4. $\phi(17 \cdot 23) = \phi(391) = 352$ e $c = 3$ (menor primo que não divide 352).

Blocos não codificados:

241 – 52 – 53 – 111 – 171 – 52 – 49 – 93 – 115 – 132 – 91 – 53 – 211

Blocos codificados:

112 – 239 – 297 – 304 – 103 – 239 – 349 – 70 – 276 – 106 – 114 – 297 – 156

1.3 Decodificação

1.3.1 Chave de Decodificação

A chave de decodificação é dada por um par de números inteiros: (n, d) , onde n é o produto dos dois primos p e q e d é o inteiro positivo inverso de c módulo $\phi(n)$.

1.3.2 Decodificando um Bloco

Se y é um bloco codificado e $D(y)$ é o bloco decodificado, então:

$D(y)$ é o resto da divisão de y^d por n .

Exemplo 1.5. $n = 391$, $c = 3$, $\phi(391) = 352$ e $d = 235$ ($d \cdot c = 705 = 2 \cdot 352 + 1$).

Blocos codificados:

112 – 239 – 297 – 304 – 103 – 239 – 349 – 70 – 276 – 106 – 114 – 297 – 156

Blocos decodificados:

241 – 52 – 53 – 111 – 171 – 52 – 49 – 93 – 115 – 132 – 91 – 53 – 211

Blocos originais:

241 – 52 – 53 – 111 – 171 – 52 – 49 – 93 – 115 – 132 – 91 – 53 – 211

Referências

COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. Rio de Janeiro: IMPA/SBM, 1997.