A MATEMÁTICA POR TRÁS DA CRIPTOGRAFIA RSA

OLIVEIRA, Cinira Aparecida de[1]; SILVA, Adriana Rodrigues da[2]
[1] Estudante do Curso de Bacharelado/Licenciatura em Matemática – UFU, Campus Santa Mônica, Uberlândia; e-mail: ciniraapoliveira@gmail.com
[2] Docente/pesquisadora da Faculdade de Matemática – FAMAT/UFU, Campus Santa Mônica, Uberlândia; e-mail: adrianafamat@ufu.br

PALAVRAS CHAVE: ALGORITMO; CONGRUÊNCIA MODULAR; CRIPTOGRAFIA RSA.

1. Introdução e Justificativa

A criptografia RSA, dentre muitas finalidades, é usada para resguardar o sigilo das diversas comunicações. É conhecido porque a chave de codificação é pública, e a chave de decodificação é privada.

O trabalho justifica-se por estudar o funcionamento da Criptografia RSA, discutindo toda a matemática necessária para a sua plena compreensão, onde são utilizados o Teorema de Euler-Fermat e o Teorema Chinês dos Restos.

2. Objetivos

- Apresentar o funcionamento da Criptografia RSA;
- Estimular o ensino da Matemática com ênfase nos fundamentos da Aritmética Modular.

3. Metodologia

Inicialmente, o trabalho consistia no estudo do material teórico. Após isso, através de um exemplo, explicou-se o processo do funcionamento do sistema RSA.

4. Resultados e discussões

Para codificar uma mensagem. basta calcular sua potência módulo *n* a um expoente escolhido. Para isso, no processo de pré-codificação, convertemos as letras da mensagem em números usando a seguinte tabela de conversão:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Os parâmetros que serão adotados são: dois primos distintos, p e q e cujo resto da divisão por 6 seja igual à 5. O valor de n será dado por $n = p.q$

Vamos considerar a palavra AMOR para fazer o processo de pré codificação, codificação e decodificação.

A mensagem será convertida no número 10222427.

Os parâmetros adotados serão $p = 17$ e $q = 23$. Portanto,

$$n = p.q = 17.23 = 391.$$

A última fase do processo de pré-codificação consiste em quebrar 10222427 em blocos menores do que $n = 391$. Assim,

$$102 - 224 - 27.$$

Para codificar a mensagem necessita-se apenas de n, que é a chave de codificação do sistema RSA.

Cada bloco é resultante do resíduo de $b^3\ por\ n$. Logo, obtemos:

$$102^3 \equiv 102^2.102 \equiv 238.102 \equiv 34(mod\ 391) \Rightarrow C(102) = 34;$$

$$224^3 \equiv 224^2.224 \equiv 128.224 \equiv 129(mod\ 391) \Rightarrow C(224) = 129;$$

$$27^3 \equiv 27^2.27 \equiv 338.27 \equiv 133\ (mod\ 391) \Rightarrow C(27) = 133.$$

Portanto, a mensagem codificada será:

$$34 - 129 - 133.$$

No processo de decodificação, é necessário estar de posse de um bloco codificado e da chave pública, para reconstruir o bloco original. O par (n, d) será chamado de chave de decodificação,

Tomando $(p-1)(q-1) = 6.k - 2$ e $d = 4.k - 1$.

Então $(p - 1)(q - 1) = 16.22 = 352 = 6.59 - 2$.

Portanto, neste caso, $k = 59$ e logo,

$$d = 4.59 - 1 = 235.$$

Tomamos que $D(34)$ é igual ao resto da divisão de 34^{235} por $n = 391$.

Temos que:

$$34 \equiv 0\ (mod\ 17),$$

$$34 \equiv 11\ (mod\ 23).$$

Assim, $34^{235} \equiv 0^{235} \equiv 0\ (mod\ 17)$.

Aplicando o Teorema de Euler-Fermat, temos:

$$11^{235} \equiv (11^{22})^{10} \,.\, 11^{15} \equiv 11^{15} (mod\ 23).$$

Mas, $11 \equiv -12 \equiv -4.3\ (mod\ 23)$ de forma que:

$$11^{235} \equiv 11^{15} \equiv -4^{15} \,.\, 3^{15}\ (mod\ 23).$$

Contudo,

$$4^{15} \equiv 1 (mod\ 23),$$

$$3^{15} \equiv 1\ (mod\ 23).$$

De modo que

$$4^{15} \equiv 2^{30} \equiv (2^{11})^2 . 2^8 \equiv 2^8 \equiv 3 (mod\ 23);$$

$$3^{15} \equiv 3^{11} \,.\, 3^4 \equiv 3^4 \equiv 12\ (mod\ 23).$$

Concluímos que

$$11^{235} \equiv -4^{15} \,.\, 3^{15} \equiv -3.12 \equiv 10\ (mod\ 23).$$

Portanto,

$$34^{235} \equiv 0\ (mod\ 17),$$

$$34^{235} \equiv 10\ (mod\ 23).$$

Aplicando o Teorema Chinês dos Restos, temos:

$$x \equiv 0\ (mod\ 17),$$

$$x \equiv 10\ (mod\ 23),$$

que resulta em

$$10 + 23y \equiv 0\ (mod\ 17) \Rightarrow 6y \equiv 7\ (mod\ 17) \Rightarrow y \equiv 3.7 \equiv 4\ (mod\ 17).$$

Portanto,

$x = 10 + 23y = 10 + 23.4 = 102.$

Aplicando o mesmo processo, obteremos os blocos decodificados:

$$102 - 224 - 27.$$

5. Considerações finais

Atualmente, a Criptografia RSA é a criptografia assimétrica mais utilizada no mundo, devido a eficácia na criptografia de dados e na segurança na quebra da chave.

6. Referências

[1] COUTINHO, S.C. **Criptografia**. IMPA, Rio de Janeiro, 2015.

[2] COUTINHO, S.C. **Números inteiros e criptografia RSA, Série de Computação e Matemática**. IMPA, Rio de Janeiro, 1997.