Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 6, n. 2, 2018.

Trabalho apresentado no XXXVIII CNMAC, Campinas - SP, 2018.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Criptografia RSA

Christopher S. Aguiar[1]
Universidade Federal de Uberlândia, UFU, Uberlândia, MG
Germano Abud[2]
Universidade Federal de Uberlândia, UFU, Uberlândia, MG

1 Introdução

A criptografia é um método de se codificar uma mensagem de modo que apenas o destinatário consiga decifrá-la. Nos últimos anos, a criptografia vem sendo uma das principais ferramentas para proteção em diversas áreas que necessitam de sigilo em relação às informações compartilhadas e os métodos evoluindo para acompanhar o rápido desenvolvimento tecnológico. Neste trabalho, apresentaremos a Cifra RSA. Este método é classificado como uma Cifra Assimétrica ou Cifra de Chave Pública [3], onde são necessárias 2 chaves distintas, a de codificação (pública) e de decodificação (privada).

2 Cifra de Chave Pública e o RSA

Para explicar o procedimento da codificação, utilizaremos um exemplo. Iremos codificar a frase: *"Quero participar do CNMAC"*.
Primeiramente escolhemos dois primos distintos, relativamente grandes, p e q, e calculamos $n = p * q$. Para ilustrar tomemos $p = 173$, $q = 229$ e, logo, $n = 39617$. O próximo passo consiste em escolher um número e que é invertível módulo $\varphi(n)$. Como $\varphi(39617) = 39216$, escolhemos $e = 85$. Logo a chave de encriptação é o par $(n, e) = (39617, 85)$. Agora a chave de decodificação é composta pelos primos escolhidos p, q e um número d, onde d é o inverso multiplicativo do e módulo $\varphi(n)$, ou seja, $d * e \equiv 1 \mod \varphi(n)$ [4]. Como o inverso de 85 é 34141, obtemos que a chave de decodificação é $(d, p, q) = (34141, 173, 229)$.

Agora, para codificar uma dada mensagem, primeiro convertemos esta mensagem em caracteres numéricos utilizando um método qualquer, como por exemplo, usar a correspondência: $A = 10, B = 11, C = 12, \cdots, Z = 35$ e para representar o espaço entre as palavras, usaremos o número 99. Aplicando este método na frase tomada como exemplo acima, obtém-se a seguinte sequência numérica:

$$26301427249925102729182510279913249912232210 12$$

[1]christopher.ufu@gmail.com
[2]germano.abud@ufu.br

Após converter a mensagem em uma sequência numérica, separe esta em blocos, de forma que o número formado em cada bloco seja menor do que n. Ressaltamos que não existe apenas uma maneira de se escolher os blocos porém cada bloco não pode começar com o dígito 0 pois caso contrário, não seria possível diferenciar o blocos $0n_1n_2$ e n_1n_2. Os blocos podem ter tamanhos variados, como por exemplo, na mensagem acima poderíamos ter 26 como o primeiro bloco e 3014 sendo o segundo bloco, tendo apenas como restrição, ser menor que n. Denotaremos cada bloco por $b_1, \cdots, b_i$, com i sendo a indexação da posição do i-ésimo bloco, e o bloco já codificado por $C(b_i)$. Separando a sequência do exemplo obtemos os seguintes blocos: $b_1 = 26301, b_2 = 4272, b_3 = 499, b_4 = 25102, b_5 = 729, b_6 = 1825, b_7 = 102, b_8 = 799, b_9 = 1324, b_{10} = 9912, b_{11} = 232, b_{12} = 21012$ e a mensagem original, convertida em números e separada em blocos, se torna:

26301.4272.499.25102.729.1825.102.799.1324.9912.232.21012

Agora para codificarmos cada bloco, usaremos a chave de encriptação e a seguinte equação:

$$b^e \equiv C(b) \mod n \tag{1}$$

Assim, para codificar o bloco b_1 resolvemos a equação $26301^{(85)} \equiv C(b_1) \mod 39617$, encontrando $C(b_1) = 13563$. Logo após repetir este procedimento para cada $C(b_i)$, enviamos a seguinte mensagem criptografada em blocos para o destinatário:

13563.23292.22862.34142.35970.18339.32909.36600.20117.6842.129.5836

Para decodificar a mensagem, o destinatário usa a chave de decodificar da seguinte maneira:

$$C(b_i)^d \equiv D(b_i) \mod n \tag{2}$$

Temos que $D(b_i) = b_i$, e isto não é difícil de se provar (ver [1]).

3 Conclusão

O RSA é muito utilizado atualmente por ser um método bastante seguro. Esta segurança provém do fato de não ser possível (com eficiência e com velocidade computacional viável), fatorar um número grande, ou seja, se o número n escolhido for grande o suficiente, se torna inviável achar os seus fatores p e q [2].

Referências

[1] S. C. Coutinho,*Números Inteiros e Criptografia RSA*. 2. ed. Rio de Janeiro: IMPA, 2011.

[2] A. V. Espina, *Números Primos e Criptografia*, Dissertação de Matemática, UNICAMP, 2014.

[3] V. M. C. Fiarresga, *Criptografia e Matemática*, Dissertação de Matemática. Faculdade de Ciências da Universidade de Lisboa , 2010.

[4] S. Singh, *O Livro dos Códigos*, (tradução). São Paulo: Editora Record, 2004.