Trabalho apresentado no XXXIX CNMAC, Uberlândia - MG, 2019.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Congruência modular e o sistema de criptografia RSA

Elber Mendes Gonçalves [1]
Discente em Licenciatura Plena em Matemática da Universidade Federal do Pará (UFPA)
Nayara do Carmo Moreira Lisboa [2]
Discente em Licenciatura Plena em Matemática da Universidade Federal do Pará
Rubenvaldo Monteiro Pereira [3]
Prof. Dr. da Universidade Federal do Pará

1 Introdução

A segurança das informações compartilhadas é fundamental, visto que, nos encontramos em meio a uma era de comunicação digital, onde em geral o compartilhamento de informações é feita por meio da internet, estando sujeitas à interceptações. Felizmente, estas informações não trafegam desprotegidas, elas são codificadas, de tal modo, que apenas seu destinatário legítmo consiga lê-las. Assim, mesmo que alguém intercepte essas informações, não conseguirá interpretá-la, pois as mesmas estão codificadas. Os processos pelos quais as informações são codificadas depende, fundamentalmente, do uso de teoria dos números com ênfase ao estudo de congruência modular.

Neste trabalho, apresentamos a congruência modular aplicada a um sistema de criptografia, o RSA e apresentaremos o funcionamento deste algoritmo através de um exemplo.

2 Como funciona o algoritmo de Criptografia do RSA

O RSA (Rivest-Shamir-Adleman) é um sistema de criptografia de chave pública criado em 1978 por R. L. Rivest, A. Shamir e L. Adleman [3]. Atualmente, o RSA é o sistema criptográfico mais utilizado na prática. O usuário que implementa esse sistema deve estar ciente que o procedimento a ser realizado pelo algoritmo do mesmo, recai a um problema específico de congruência modular, o cálculo do resíduo de potências.

O algoritmo do RSA funciona da seguinte forma: escolha dois números primos, p e q e calcule seu produto $n = p \times q$. Escolha um número, $e \in \mathbb{N}$, tal que $1 < e < \varphi(n)$ e $mdc[e, \varphi(n)] = 1$, onde $\varphi(n)$ é a função totiente de Euler. Calcule d, tal que d seja a classe inversa de e módulo $\varphi(n)$ [1]. Os números n, e e d formam pares de chaves que são usadas para codificarmos e decodificarmos informações, por meio das respectivas regras:

[1] elbermnds@gmail.com
[2] nayaracmlisboa@gmail.com
[3] rubenvaldop@yahoo.com.br

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

$$a^d \equiv b(mod.n) \tag{2}$$

Ao par (e, n) chamamos de chave pública e ao par (d, n) de chave privada. Os fatores p e q podem ser mantidos em segredo com a chave privada. Atualmente, é difícil obtermos a chave privada d da chave pública (n, e), pois seria necessário fatorar n, encontrando seus fatores p e q que são primos suficientemente grandes, o que torna a tarefa de fatorar n inviável.

A seguir denotemos o uso desse algoritmo. Vamos agora, codificar o nome NAYARA e decodificá-lo em seguida. O primeiro passo a ser feito é transformar o nome NAYARA em código ASCII: 110 97 121 97 114 97. Escolhendo p e q, respectivamente, 13 e 17, obtemos $n = 13 \times 17 = 221$ e $\varphi(n) = 192$. Em seguida, tomemos $e = 5$, logo dispomos do par $(5, 221)$ e com o mesmo, codificamos a mensagem em: 145 54 49 54 173 54. Para a decodificação, o usuário final necessita do par (d, n). Neste caso, $d = 77$, logo temos o par $(77, 221)$ para decodificarmos a mensagem em: 110 97 121 97 114 97, que é a representação do nome NAYARA em código ASCII.

3 Conclusão

Dado o exposto, apresentamos o algoritmo do RSA e seu funcionamento, onde o processo realizado por tal recai a um problema específico de congruência modular, portanto, faz-se necessário este conceito matemático para, assim, codificarmos e decodificarmos informações através deste sistema, visto que, codificar uma informação por meio do RSA é o mesmo que calcular o resíduo de uma potência, que consiste em um problema de congruência modular. Além disso, sugere-se o conhecimento matemático necessário ao funcionamento de sistemas criptográficos como o RSA, criado especificamente com o intuito de manter sigilo de informações compartilhadas entre usuários.

Dessa maneira, os tópicos abordados nesse trabalho visaram a importância da segurança de informações que trafegam pela internet e que estão sujeitas à interceptações por terceiros.

Referências

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

[2] S. C. Coutinho. *Números Inteiros e Criptografia*. Série de Computação e Matemática. Rio de Janeiro, Sociedade Brasileira de Matemática e Instituto de Matemática Pura e Aplicada, 1997.

[3] R. L. Rivest, A. Shamir, L. A. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *CACM*, 121, P. 120-126, 1978.