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

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Criptografía: um estudo dos métodos e aplicação em Phyton

Michael Dayves Pereira Pimenta [1]
Prof. Dr. Rafael Peixoto [2]

1 Introdução

Desde tempos antigos a humanidade desenvolveu técnicas para se comunicar de maneira secreta, escondendo conteúdos com teor confidencial de terceiros a quem não são destinados. Essas técnicas são parte de uma ciência que busca tornar esse processo mais seguro possível, a criptografia, que por sua vez engloba as formas de cifragem e decifragem de uma mensagem. Hoje em dia, vemos que a criptografia ainda é presente em nosso mundo e seus métodos estão muito mais sofisticados e seguros, por isso buscamos aplicá-los a uma linguagem de programação, no caso o Phyton e além disso estudar e compreender a modelação matemática presente em cada processo de cifragem com o propósito de criar um laço tecnológico envolvendo o conteúdo histórico presente em algumas cifras.

2 Desenvolvimento

Durante a pesquisa, buscamos estudar diversas cifras e métodos de cifragem, que foram dividas com relação a caracteristica do método e o tipo do processo utilizado, a seguir temos algumas cifras e o processo matemático associado:

2.1 Cifra de Vigenère

A cifra de Vigenère utiliza uma técnica denominada polialfabética, onde um caractere pode ser criptografado em diferentes símbolos, dependendo de sua posição na mensagem. Diferentemente da cifra utilizada por César ou a técnica do Atbash, segundo [1] ela proporcionou mais segurança na troca de informações por não ter uma frequência perceptível das letras. O processo de cifragem consiste em substituir cada letra da mensagem original por outra que fica em uma posição definida pela chave que é escolhida e estruturada por quem vai enviar a mensagem.

[1] Michaeldayves@gmail.com
[2] rafael.peixoto@uftm.edu.br

2.1.1 Processo matemático associado

Primeiro associa-se as letras do alfabeto aos números $a = 0$, $b = 1$,..., $z = 25$. Depois define-se a chave que será utilizada de maneira que ainda associando as letras ao números é construída como, por exemplo, a chave K:

$$K = (1, 2, 0) = (b, c, a) \tag{1}$$

Se x pertence a $\mathbb{Z}_{25}$ a função que cifra o primeiro caractere x_1 do texto original é:

$$c(x_1) \equiv (x_1 + K_1) \pmod{26} \tag{2}$$

A relação presente nesse tipo de cifra é a de congruência. Para o caso da mensagem ser maior que a chave, os caracteres que sobram tem a operação efetuada com a chave retornando ao primeiro termo. Criptografando a letra a da palavra $math$, usando a chave (1), na equação (2) por exemplo:

$$c(a) \equiv (a + 2) \bmod(26)$$

$$c(0) \equiv (0 + 2) \bmod(26)$$

$$c(0) = 2 \text{ , i.e., } c(a) = c.$$

2.2 Cifra de Hill

Para se aplicar a técnica de Hill, escolhe-se uma matriz quadrada, cujas entradas K_{ij} são números inteiros em $\mathbb{Z}_{25}$. Esta matriz é a chave do método e dado um texto x a ser criptografado, deve-se quebrá-lo em segmentos de n caracteres como: $x_1x_2x_3x_4...x_n$. Em seguida multiplicamos a matriz quadrada pela matriz coluna de x obtendo os termos criptografados em forma de matriz que são dispostos numa lista onde se substitui os números pelas letras.

Exemplo de matriz chave 3×3 e a operação envolvida na cifra:

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

.

2. Aplicação em Phyton

Após o estudo das cifras, buscamos implementar sua utilização usando a linguagem de programação Phyton, com isso obtivemos sucesso, uma vez que foi criado um fluxograma e o algoritmo baseado nos laços que a criptografia das cifras requerem.

Referências

[1] A. C. Faleiros, - *São Carlos, SP : SBMAC, 2011, 138 p., (Notas em Matemática Aplicada)*

