I Workshop de Álgebra da UFG – CAC

Criptografia

Géssica Cristina dos Reis
Laura Thais Lourenço
Bruno Castilho Rosa
Lucas Borges de Faria
Igor dos Santos Lima (Orientador)

Resumo

- A Criptografia é um ramo da Matemática que lida com princípios de escrever em cifras ou códigos, utilizando um conjunto de técnicas que transforma arquivos legíveis em algo ilegível.
- A Criptografia trabalha com "chave secreta", que é um pedaço de informação que controla a operação de um algoritmo de criptografia. Há dois tipos de chaves criptográficas: chaves simétricas e chaves assimétricas.
- Existem vários códigos na criptografia em que fazem uso da matemática, entre eles o código Cifra de César, que representa também um criptossistema.
- Neste trabalho, abordaremos o código Cifra de César, que é um caso particular de um teorema que garante a existência de um criptossistema.

Preliminares

- Na Criptografia a mensagem a ser enviada é chamada de texto-original e a mensagem codificada passa a ser chamada de texto-cifrado. No processo de converter um texto-original em um texto cifrado é conhecido como codificação, e o processo de reverter são chamados de decodificação ou cifragem. A escrita do texto-original e do texto-cifrado é composta por símbolos de um determinado alfabeto K (letras e símbolos).
- O texto original e texto cifrado são divididos em mensagens unitárias, onde esta mensagem poderá ser um bloco do alfabeto K. Assim, o processo de codificação é uma função que associa cada mensagem unitária x do texto original a uma mensagem unitária c do texto cifrado.
- Considere M o conjunto de todas as possíveis mensagens unitárias x do texto original e C o conjunto de todas as possíveis mensagens unitárias c do texto cifrado. Então o processo de codificação é dado pela função bijetora abaixo:
- $f: M \to C$ tal que $f(x) = c$.
- Como essa função possui inversa, então o processo de decodificação será dado pela seguinte função:
- f^{-1}: C → M tal que f^{-1} (c) = x.
- Assim, um criptossistema será representado por qualquer bijeção de M em C:
- $M \xrightarrow{f} C \xrightarrow{f^{-1}} M$.
- É usual substituirmos os símbolos de um alfabeto K por números inteiros $\mathbb{Z}$, de forma que possamos obter uma correspondência entre K e $\mathbb{Z}_{27}$.
- K = {A, B, C,...,, X,Y,Z, espaço = u} e $\mathbb{Z}_{27}$ = {0,1,2, ..., 25,26}
- Com isso formamos a seguinte tabela 1:
- $\begin{matrix} A & B & C & \cdots & X & Y & Z & u \\ \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0 & 1 & 2 & \cdots & 23 & 24 & 25 & 26 \end{matrix}$
- **Teorema 1.** Sejam n ∈ $\mathbb{N}$ e a, b ∈ $\mathbb{Z}_n$ fixados. Se o mdc (a, n) = 1, então a função:
- f: $\mathbb{Z}_n \to \mathbb{Z}_n$ dada por $f(x) = ax + b$.
- é um criptossistema.
- **Observação 1.1** Seja $f(x) = ax + b$ um criptossistema. O par (a,b) é chamado de chave secreta. Se n = 27, $a = 1$ e $b \in \mathbb{Z}_{27}$ então o criptossistema:
- $f(x) = x + b$.
- é denominado Cifra de César.

Resultados

- Primeiramente demonstraremos o **Teorema 1.**
- **Prova:** Sendo o mdc $(a,$ n) = 1 temos que existe $a' = a^{-1} \in \mathbb{Z}_n^*$ tal que $a \,.\, a' = 1$.
- Assim:

$f^{-1}(x)$=a'x+b',
onde $b' = a'\, b$ é tal que
$f \circ f^{-1} = f^{-1} \circ f = I_{\mathbb{Z}_n}$;
isto é , f^{-1} é a função inversa *f.*
Exemplo de uma aplicação do código Cifra de César.
1. Seja *f:* $\mathbb{Z}_{27} \to \mathbb{Z}_{27}$ dada por *f(x)=x+4* uma Cifra de César. Suponha que o emissor irá enviar a mensagem "Guerra" de forma codificada. Então conforme a Tabela 1 tem-se a seguinte correspondência:

G	→	$f(G) = f(6) = 10$	= K
U	→	$f(U) = f(20) = 24$	= Y
E	→	$f(E) = f(4) = 8$	= I
R	→	$f(R) = f(17) = 21$	= V
R	→	$f(R) = f(17) = 21$	= V
A	→	$f(A) = f(0) = 4$	= E

Logo o receptor irá receber a seguinte mensagem: KYIVVE. Ao receber a mensagem, o receptor irá aplicar a operação inversa em cada letra da mensagem.
Onde a função inversa é dada por:
f^{-1} =y-4.
Exemplo:
$f^{-1}(K)$ = 10-4=6 = G.
$f^{-1}(Y)$ = 24-4=20 = U.
...
E assim sucessivamente até repor a mensagem original completa: **GUERRA**

Conclusão

- Neste artigo relatamos um pouco da Criptografia, onde vimos uma ligação entre essa ciência e a Matemática. O código cifra de César, o qual trabalhamos acima é um dos códigos mais simples na Criptografia, porém para que se tenha segurança no envio das mensagens é necessário códigos mais complexos, de modo que apenas o receptor consiga decifrá-la.

Referências

- FRANÇA, W. B. A. Criptografia.
- SILVA, A. A. Números, Relações e Criptografia.

* A impressão deste foi financiada pela FAPEG .