VI SEMANA UNIVERSITÁRIA DA URCA
XXIV SEMANA DE INICIAÇÃO CIENTÍFICA DA URCA
13 a 17 de Dezembro de 2021
Tema: "Centenário de Paulo Freire: contribuição da divulgação científica e tecnológica em defesa da vida, da cidadania e da educação"

INTRODUÇÃO A CRIPTOGRAFIA SIMÉTRICA

Sabrina Bento Pereira[1], José Augusto Pereira Nogueira[2]

Resumo: No mundo moderno das comunicações, o envio de dados de todos os tipos é realizado frequentemente e para que essas informações, que muitas vezes são pessoais, não caiam em mão erradas, foi desenvolvida a Criptografia. Este trabalho apresenta uma pesquisa sobre criptografia simétrica e algumas de suas diferentes formas de cifragens e suas aplicações. O objetivo do artigo é demostrar de forma didática as cifras abordadas e sua integração com a matemática básica, contextualizando seus fatores históricos e evidenciando a importância da matemática neste processo. Para tanto, o trabalho discorre sobre as cifras de substituição, transposição e por meio do uso de matriz. Por fim, daremos exemplos que permitirá identificar qual o método de cifragem mais seguro na criptografia simétrica.

Palavras-chave: Cifras. Criptografia. Criptografia Simétrica.

1. Introdução

A criptografia é a ciência responsável em investigar os métodos para codificar uma mensagem de forma que só o receptor legítimo consiga interpretá-la. Este método de segurança é estudado desde a antiguidade e já existe há alguns séculos, ao longo do tempo esta foi sendo desenvolvida chegando a que conhecemos hoje, a criptografia que utiliza o sistema de chaves criptográficas.

Nas últimas décadas proteger informações se tornou cada vez mais necessário. Com o surgimento da internet e com a disponibilidade de computadores, as técnicas utilizadas na criptografia se tornaram mais eficientes e acessíveis, deixando os métodos conhecidos como decifração resultassem em algo antiquado, assim, foi indispensável recorrer ao desenvolvimento de novas técnicas que permitiam garantir a segurança da transação de dados entre dispositivos digitais. Dessa forma, a criptografia torna-se um agente de segurança em um sistema de comunicações.

Atualmente utiliza-se para segurança do trânsito digital a Criptografia com o sistema de chaves criptográficas, estas chaves consistem em um conjunto de bits (digito binário) baseado em um algoritmo capaz de decodificar a informação. A criptografia é dividida em dois tipos: simétrica e assimétrica.

A criptografia simétrica, conhecida por ser a mais simples, utiliza uma mesma chave para o remetente e destinatário na codificação e decodificação da mensagem. Algoritmos que utilizam a criptografia simétrica são mais rápidos, uma vez que a utilização de apenas uma chave entre emissor e receptor simplifica o processo de criptografia, contudo não são tão seguros quanto os algoritmos de criptografia assimétrica.

1 Universidade Regional do Cariri, email: sabrina.bento@urca.br
2 Universidade Regional do Cariri, email: augusto.nogueira@urca.br

A criptografia assimétrica utiliza um par de chaves, uma pública e uma privada, onde, o código público criptografa e o privado descriptografa. Esse processo torna o envio de dados mais seguro. Esse tipo de encriptação tende a ser mais lento, pois, com a possibilidade de trabalhar com diferentes emissores da mensagem necessita-se de um poder computacional maior que o dos algoritmos de chave simétrica.

Nosso trabalho abordará a criptografia simétrica abordando seus principais métodos de codificação e decodificação, relacionando seu desenvolvimento com a matemática, tendo como referência estudos bibliográficos da área da pesquisa. O estudo realizado é necessário e norteador para o desenvolvimento da nossa próxima pesquisa a respeito da criptografia assimétrica.

2. Objetivo

Este trabalho tem como objetivo apresentar as diferentes formas de cifragem da criptografia simétrica, e sobretudo, enfatizar a dependência e a relação desse método criptográfico com a matemática.

3. Metodologia

A pesquisa foi desenvolvida através de pesquisas bibliográficas sobre a área de estudo abordada, através de artigos e materiais dispostos na internet.

4. Resultados

De acordo com Cavalcante (2004) a criptografia simétrica foi o primeiro tipo de criptografia desenvolvido. Funciona transformando um texto em uma mensagem cifrada, por meio da definição de uma chave secreta, que será utilizada posteriormente para decriptar a mensagem, tornando novamente um texto simples

Este tipo de criptografia se caracteriza por usar funções matemáticas mais simples e por isso ser mais rápida, como desvantagem, não só o transmissor deve conhecer a chave como também o receptor. Além disso, o volume total dos dados transmitidos é limitado pelo tamanho da chave.

- **Métodos de Criptografia Simétrica**

Na criptografia simétrica é utilizado dois métodos: as cifras de **substituição e transposição.** O método de substituição realiza o processo de troca de caracteres, bits ou blocos por diferentes caracteres, bits ou blocos. Na transposição a ordem dos caracteres, bits ou blocos são alteradas.

- **Cifras de Substituição**

Uma cifra de substituição é um tipo de criptografia em que caracteres ou unidades de texto são substituídos por outros para criptografar uma sequência de texto. Cada grupo de letras é substituído por outro grupo de letras.

Na Tabela 1 é mostrado um exemplo simples para compreensão da ideia repassada. Cada uma das 26 letras do alfabeto tem um correspondente uma outra letra.

Tabela 1: Cifras de Substituição

a	b	c	d	e	f	g	h	i	j	k	l	m
K	L	O	P	B	M	G	Z	N	T	C	H	W
n	o	p	q	r	s	t	u	v	w	x	y	z
D	S	Y	V	U	R	Q	X	A	E	G	I	J

Esse método é conhecido como cifras de substituição. Substituindo as letras da palavra "teorema" pelas suas letras correspondentes resultaria em "QBSUBWK".

A Cifra de substituição apesar de útil, quando é uma pequena frase pode ser descoberta facilmente, como, observando as repetições de prováveis vogais, M antes de P e B e outros fatores comum na formação de frases. Observando alguns detalhes, a mensagem tem muitas chances de ser descriptografada por qualquer pessoa e não somente pelo receptor.

- **Cifras de Transposição**

Após o método de substituição estar fragilizado, foi desenvolvido o método de transposição. Nesta Cifra o texto permanece o mesmo, contudo, a ordem dos caracteres é alterada, assim, embaralhando a mensagem de acordo com um determinado padrão.

A ordem da leitura pode ser determinada também por uma palavra-chave, que definirá a largura da matriz. Observe na tabela 2 por exemplo, considere a chave sendo a palavra teoria e a mensagem de texto "Você pode ir me ver hoje na rua?", enumeramos as letras da palavra chave em ordem crescente alfabética, assim servindo de apoio para enumerar as colunas, ficando 624531.

Tabela 2: Cifras de transposição

t	e	o	r	i	a
6	2	4	5	3	1
v	o	c	e	p	o
d	e	i	r	m	e
v	e	r	h	o	j
e	n	a	r	u	a

A codificação da mensagem fica de acordo com a ordem crescente dos números no topo de cada coluna. Assim, a informação será transmitida da seguinte forma, "oejaoeenpmonciraerhrvdve".

- **Matriz**

Outra maneira de codificar uma mensagem utilizando a criptografia é por meio de multiplicação da matriz. É necessário, uma matriz chave e sua inversa, uma tabela com associação das letras do alfabeto aos números e a mensagem que se deseja enviar. A segurança da mensagem torna-se muito alta com o método da matriz. Na tabela 3 e nos cálculos das matrizes é mostrado o método de codificação da mensagem "Eu andarei pela cidade" através do uso da matriz.

Tabela 3: Método pela Matriz

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	2	3	4	5	6	7	8	9	10	11	12	13	14
O	P	Q	R	S	T	U	V	W	X	Y	Z	*	-
15	16	17	18	19	20	21	22	23	24	25	26	27	-

Para decodificação por meio da matriz é necessário inicialmente o receptor e o emissor ter acesso a matriz chave. Suponha a matriz C abaixo como a matriz chave e considere sua inversa como chave para decodificação da mensagem.

$$C = \begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix} \Rightarrow C^{-1} = \begin{bmatrix} 7 & -3 \\ -2 & 1 \end{bmatrix}$$

O remetente deve conhecer a tabela com seus respectivos números correspondentes. Codificando a mensagem original "Eu andarei pela cidade", resulta na seguinte matriz.

$$\mathrm{M} = \begin{bmatrix} 5 & 21 & 27 & 1 & 14 & 4 & 1 & 18 & 5 & 9 & 16 \\ 5 & 12 & 1 & 27 & 3 & 9 & 4 & 1 & 4 & 5 & 0 \end{bmatrix}$$

Multiplicando a matriz M, pela Matriz chave C, obtém-se a matriz que será enviada ao receptor.

$$\mathrm{M}\times\mathrm{C} = \begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix} \times \begin{bmatrix} 5 & 21 & 27 & 1 & 14 & 4 & 1 & 18 & 5 & 9 & 16 \\ 5 & 12 & 1 & 27 & 3 & 9 & 4 & 1 & 4 & 5 & 0 \end{bmatrix}$$

$$\mathrm{MC} = \begin{bmatrix} 20 & 57 & 30 & 82 & 23 & 31 & 13 & 21 & 17 & 24 & 16 \\ 45 & 126 & 61 & 191 & 49 & 71 & 30 & 43 & 38 & 53 & 32 \end{bmatrix}$$

A matriz MC é transmitida ao receptor que deve usar a matriz C^{-1} para que possa descriptografar a mensagem. Ficando $C^{-1}MC = M$

$$C^{-1}MC = \begin{bmatrix} 7 & -3 \\ -2 & 1 \end{bmatrix} \times \begin{bmatrix} 20 & 57 & 30 & 82 & 23 & 31 & 13 & 21 & 17 & 24 & 16 \\ 45 & 126 & 61 & 191 & 49 & 71 & 30 & 43 & 38 & 53 & 32 \end{bmatrix}$$

$$M = \begin{bmatrix} 5 & 21 & 27 & 1 & 14 & 4 & 1 & 18 & 5 & 9 & 16 \\ 5 & 12 & 1 & 27 & 3 & 9 & 4 & 1 & 4 & 5 & 0 \end{bmatrix}$$

A matriz volta a sua mensagem original após ser multiplicado pela inversa da matriz chave. Por fim, reverte-se os números em letras utilizando a tabela.

5. Conclusão

Neste artigo foi apresentado a técnica de criptografia simétrica. Foram utilizadas três abordagens diferentes de cifragem. A primeira consistia em gerar uma mensagem codificada através da substituição de caracteres, considerado a cifragem com o nível de segurança baixo, a segunda tem como base a substituição, mas, trabalha com a transposição dos dados, embaralhando a mensagem que se deseja enviar, a última cifra aborda o estudo de matrizes, é necessário conhecimento matemático para descriptografar a mensagem, e tornar a cifragem mais segura.

Os métodos foram testados e ficou explicito de forma clara a cifragem com mais segurança. Este processo de criptografia envolve cálculos mais simples, por isso a criptografia simétrica se torna mais rápida. Apesar da criptografia simétrica atualmente não ser o método mais seguro, foi o início do desenvolvimento tecnológico altamente ligado aos conceitos matemáticos.

6. Agradecimentos

Agradecemos a URCA e aos recursos de financiamento do FECOP pela concessão da bolsa do Programa Institucional de Bolsas de Iniciação Científica (PIBIC).

7. Referências

CAVALCANTE, A.L.B. **Matemática II. Notas de Aula**. Brasília: Editora UPIS (2004).

CAVALCANTE, A.L.B. Teoria dos Números e Criptografia. SCRIBD.2014. Disponível em:< https://scribd.com/document/51376255/teoria-dos-n-meros-e-criptografia Acesso em: 28 out.2021

FERNANDO. Matrizes e Criptografia. **A Educação Matemática**. Disponível em: <A EDUCAÇÃO MATEMÁTICA: MATRIZES E CRIPTOGRAFIA (educacaomatematica2010.blogspot.com)> Acesso em: 30 out. 2021.