

UNIVERSIDADE FEDERAL DO AMAZONAS

FACULDADE DE TECNOLOGIA

ENGENHARIA DA COMPUTAÇÃO

**GRUPO 4 - CRIPTOGRAFIA**

# Criptografia: Computação e Aplicações de Álgebra Linear

**Manaus**

**2023**

UNIVERSIDADE FEDERAL DO AMAZONAS

FACULDADE DE TECNOLOGIA

ENGENHARIA DA COMPUTAÇÃO

**FABRÍCIO FILHO, LAYSA SIQUEIRA, JÚLIO MELO, MARINALDO JÚNIOR E REBECA AGRA**

# Criptografia: Computação e Aplicações de Álgebra Linear

Projeto apresentado ao curso de engenharia da computação, como parte dos requisitos necessários à obtenção do nota de Álgebra Linear II, ministrada pela professora Karla Tribuzy.

Manaus

2023

## Resumo

**Palavras-chave:**

## Abstract

**Keywords:**

## Sumário

1. [Introdução 9](#_TOC_250002)
2. Referencial Teórico
3. Metodologia 12
4. Resultados e Discussão 15
5. [Conclusão 17](#_TOC_250000)

## Introdução

A criptografia está em contato diariamente com a sociedade, e ela é muito importante no contexto de segurança ou privacidade, ela está em constante contato com tudo em nossa volta, de mensagens até proteção de contas bancárias. A criptografia surgiu durante a segunda guerra mundial no qual era essencial manter informações secretas e prevenir possíveis ataques, atualmente a criptografia evoluiu principalmente no meio computacional na qual se usa um sistema de chaves criptográficas, que consiste em conjunto de bits baseados em determinado algoritmo capaz de decodificar a informação. A matemática é de grande importância tanto para criptografia quanto para computação porque conseguimos levar esses problemas pro âmbito matemático e conseguimos solucioná-los com mais facilidades. É possível usar Álgebra Linear na criptografia como um método para solucionar problemas através de matrizes.

Essa dissertação se propõe a fazer um estudo sobre criptografia usando aplicações de Álgebra Linear solucionando questões, a ideia é que conseguimos entender como funciona tais aplicações para enriquecer nosso conhecimento e obter excelentes resultado nesse estudo, nesse contexto usaremos Cifras de Hill que é um tipo de cifra de substituição baseado em álgebra linear usado para codificação de mensagens, também usaremos aplicações algébricas como multiplicações de matrizes, matrizes simétricas e transformações usando modulo resíduo que serão mais aprofundadas ao longo do artigo.

Como acadêmicos de Engenharia da Computação, criaremos um código computacional que visa codificar ou descodificar palavras usando alguns das aplicações citadas acima, tal programa será estudado e mostraremos como a criptografia e Álgebra Linear trabalhadas em conjunto são abordados na computação visando sempre no aprendizado.

**Referencial Teórico**

**A CRIPTOGRAFIA COMO UMA APLICAÇÃO DA TEORIA DE ÁLGEBRA LINEAR**

A criptografia é a utilização de códigos secretos para garantir a segurança na comunicação e proteger informações sigilosas. Ao longo da história, a criptografia tem sido usada em diferentes contextos, desde a Grécia antiga até os dias atuais.

Com o surgimento da globalização e a expansão da internet, a criptografia tornou-se ainda mais importante, pois é necessária para garantir a transmissão segura de dados pela rede.

O objetivo desse trabalho é explicar um método específico da Criptografia: As Cifras de Hill, que foi inventado em 1929 por Lester S. Hill. O presente trabalho mostra como é composto esse método, suas etapas de codificação e decodificação.

Para explicar o procedimento de codificação das Cifras de Hill, é necessário basear-se em ferramentas da Álgebra Linear e da Aritmética Modular. Da Álgebra Linear são utilizadas as matrizes e operações matriciais (multiplicação de matrizes e conhecimentos a respeito de matrizes inversas). Além de conceitos sobre independência linear e transformações lineares. A seguir, alguns conceitos da Aritmética Modular utilizado nesse trabalho:

Definição 1: Dado um número inteiro positivo m e dois inteiros a e b quaisquer, dizemos que a é equivalente a b módulo m, e escrevemos a = b(mod m) se a – b é um múltiplo inteiro de m. Dado um módulo m, qualquer inteiro a é equivalente, módulo m, a exatamente um dos inteiros 1,2,...,m-1,0. Esse inteiro é chamado o resíduo de a módulo m e {1,2,...,m-1,0} = Zm é o conjunto dos resíduos de a módulo m.

Definição 2: Dado um número inteiro a em Zm, dizemos que um número 1-a em Zm é um inverso multiplicativo de a módulo m se a\*(1-a) ≡ 1 (mod m).

O processo de cifras de Hill consiste em transformar pares sucessivos de texto em texto cifrado, através da escolha de uma matriz 2x2 A, e uma tabela com valores numéricos para todas as letras do alfabeto. Cada par de letras do texto se transforma em um vetor-coluna p através do seu correspondente valor numérico, e o produto Ap é convertido em seu equivalente alfabético. Como o alfabeto possui 26 letras, e a multiplicação de Ap pode resultar em um vetor coluna com números maiores que 26, é utilizado a teoria dos conjuntos dos resíduos módulo 26 para fazer a correspondência da tabela.

O processo de decodificação que tem que ser realizado pelo receptor é semelhante ao de codificação, com apenas uma diferença, usa-se a inversa da matriz de codificação na multiplicação pelas matrizes colunas dos pares de letras do texto codificado.

**Metodologia**

Este trabalho é de natureza descritiva com uma abordagem quantitativa, pois visa solucionar as questões propostas cruzando com toda a pesquisa bibliográfica já feita. O estudo parte de materiais bibliográficos coletados online, sendo dois artigos abordando a aplicabilidade de métodos algébricos na criptografia. Analisando as questões, foi utilizado principalmente o processo de cifras de Hill e cifras de substituição que se baseiam em transformações matriciais, ambos foram aplicadas por estarem enquadradas como conteúdos essenciais para a resolução das problemáticas.

**Resultados**

Questão 6 – HPAFQGGDUGDOHPGODYNOR

C =

(8,16,1) (6,17,7) (7,4,21)

Criptografado

IHA VEC OME

(9,8,1) (22,5,3) (15,13,5) P =

Descriptografado

1° L3 • 5 =

2° = (mod 26)

3° = L2 • 15

4° =

5° L1 • 19 =

6° =

7° =

→A-1= (Matriz chave decodificada)

|  |  |  |
| --- | --- | --- |
| H | P | A |
| 8 | 16 | 1 |

|  |  |  |
| --- | --- | --- |
| F | Q | G |
| 6 | 17 | 7 |

|  |  |  |
| --- | --- | --- |
| G | D | U |
| 7 | 4 | 21 |

|  |  |  |
| --- | --- | --- |
| H | P | G |
| 8 | 16 | 7 |

|  |  |  |
| --- | --- | --- |
| O | D | Y |
| 15 | 4 | 25 |

|  |  |  |
| --- | --- | --- |
| G | D | D |
| 7 | 4 | 4 |

|  |  |  |
| --- | --- | --- |
| N | O | R |
| 14 | 15 | 18 |

I HAVE COME TO BURY CAESAR

Questão 8 –

Assim como em matrizes quaisquer, uma matriz só admite inversa se, e apenas se, seu determinante for diferente de zero.

Ex: = → det = (1 - 0) – (27 - 0) = 0 – 0 = 0 (mod 29)

Se:

• =

=

→ a = 1 e b = 0 X

→ a = 0 e b = 1/27

Não é invertível.

•Logo, a matrtiz cuja as entradas Z29 se, se apenas se o det(Z29 ) ≠ 0 com (mod 29).

Questão T1 –

S9 = {a1,a2,a3,...,a6} = {1,2,4,5,7,8}

a)

* S2 = {1}
* S3 = {1,2}
* S4 = {1,3}
* S5 = {1,2,3,4}
* S6 = {1,5}
* S7 = {1,2,3,4,5,6}
* S8 = {1,3,5,7}
* S9 = {1,2,4,5,7,8}
* S10 = {1,3,7,9}
* S11 = {1,2,3,4,5,6,7,8,9,10}
* S12 = {1,5,7,11}
* S13 = {1,2,3,4,5,6,7,8,9,10,11,12}
* S14 = {1,2,3,5,9,11,13}
* S15 = {1,2,4,7,8,11,13,14 }

-Somatório

– Conjecturas

•Caso n seja primo, então Sn vai ser o conjunto de todos os números de 1 até (n-1). Ou seja, todos estes são relativamente primos a n.

•O somatório de Sn sempre vai resultar em um múltiplo de n. Assim, aplicando o (mod n) nos somatórios, sempre resultará em zero.

\*Todas as conjunturas acima se aplicam em todo n>2, ou seja, também em n>15.

b)

P2 = [1]; Det P2 = 1; Det P2(Mod 2) = 1

P3 = ; Det P3 = 3; Det P3(Mod 3) = 0

P4 = ; Det P4 = -8; Det P4(Mod 4) = 0

P5 = ; Det P5 = 160; Det P5(Mod 5) = 0

P6 = ; Det P6 = -24; Det P6(Mod 6) = 0

P7 = ; Det P7 = -272; Det P7(Mod 7) = 0

P8 = ; Det P8 = 2048; Det P8(Mod 8) = 0

P9 = ; Det P9 = -177147; Det P9(Mod 9) = 0

P10 = ; Det P10 = 5760; Det P10(Mod 10) = 0

P11 = ;

Det P11 = 5500000000; Det P11 (Mod 11)= 0

P12 = ; Det P12 = 13824; Det P12(Mod 12) = 0

P13 = ;

Det P13 = 4829554409472; Det P13(Mod 13)= 0

P14 = ; Det P14 = -412878; Det P14(Mod 14) = 0

P15 = ;

Det P15 = 1085767680; Det P15(Mod 15) = 0

– Conjecturas

Todos os módulos das matrizes a partir de n=3 são iguais a zero.

c)

Aplicando o teorema 2.2.3 na matriz P5 temos:

P5 =

Somando todas as linhas e substituindo a última com o resultado de cada elemento, somando temos:

P’5 = ;

•Ou seja, o resultado de cada soma os elementos, é igual ao somatório propriamente dito do conjunto S5.

•Logo a sua determinante também é igual a determinante de P5, como também seu módulo é igual a zero, comparando o teorema.

det P’5 = det P5 = 160

•Ao inverter qualquer matriz Pn, o resultado sempre será divido por um número em comum, sendo este um múltiplo de n.

=

**Discussão**

## Conclusão

Este trabalho é de natureza descritiva com uma abordagem quantitativa, pois visa solucionar as questões propostas cruzando com toda a pesquisa bibliográfica já feita. O estudo parte de materiais bibliográficos coletados online, sendo dois artigos abordando a aplicabilidade de métodos algébricos na criptografia. Analisando as questões, foi utilizado principalmente o processo de cifras de Hill que é realizada multiplicando-se cada bloco de letras por uma matriz chave invertível e cifras de substituição que utiliza funções (f(x)), onde o texto original é representado por uma variável x, ambos foram aplicadas por estarem enquadradas como conteúdos essenciais para a resolução das problemáticas.

Logo, com base na resolução dos exercícios e utilizando aspectos da programação ao desenvolver um algorítimo baseado nas cifras de Hills, concluímos que foi de suma importância aprender e utilizar na prática ensinamentos de Algebra Linear para solucionar problemas do cotidiano, como enviar mensagens criptografadas para destinatários desejados, dificultando ao máximo a vinda de usuários indesejados que não fora autorizados a receber a mensagem, mostrando a importância da matemática e suas devidas aplicações na hora de implementar aspectos da criptografia.

**Referências Bibliográficas**

SBPC – Sociedade Brasileira para o Progresso da Ciência. Disponível em: <http://www.sbpcnet.org.br/livro/68ra/resumos/resumos/5747_16728345cb8c41053d3264c73ee64d4fc.pdf>. Acesso em: 30 mai. 2023.

CRIPTOGRAFIA DE DADOS UTILIZANDO MATRIZES | RE3C - Revista Eletrônica Científica de Ciência da Computação. Disponível em: <https://revistas.unifenas.br/index.php/RE3C/article/view/100>. Acesso em: 30 mai. 2023.

ABCM. Disponível em: [https://www.abcm.org.br/anais/creem/2012/A%20CRIPTOGRAFIA%20COMO%20UMA%20APLICAÇÃO%20DA%20TEORIA%20DE%20ÁLGEBRA%20LINEAR.pdf](https://www.abcm.org.br/anais/creem/2012/A%20CRIPTOGRAFIA%20COMO%20UMA%20APLICA%C3%87%C3%83O%20DA%20TEORIA%20DE%20%C3%81LGEBRA%20LINEAR.pdf). Acesso em: 30 mai. 2023.

CRIPTOGRAFIA: quando e como surgiu e onde é usada. Disponível em: <http://blog.mastermaq.com.br/como-surgiu-a-criptografia/>. Acesso em: 26 jun. 2023.