

# Cifra de Hill: Aplicações e Fundamentos Matemáticos na Criptografia.

Julia Monteiro<sup>1</sup>

PPG-CompMat/UERJ, Rio de Janeiro, RJ

**Resumo** Este trabalho explora a interseção entre criptografia e álgebra linear, destacando como conceitos matemáticos fundamentais são utilizados para proteger informações no ambiente digital. Um dos focos principais é a Cifra de Hill, um método de criptografia que aplica operações de álgebra linear para codificar e decodificar mensagens. Utilizando matrizes e multiplicação vetorial, a Cifra de Hill transforma o texto original em um texto cifrado que é difícil de decifrar sem a chave correta. Serão abordados os princípios matemáticos por trás da Cifra de Hill, suas vantagens e limitações, e exemplos práticos de como ela opera.

**Palavras-chave.** Criptografia, Cifras de Hill, Álgebra Linear, Matrizes.

**Abstract.** *This work explores the intersection between cryptography and linear algebra, highlighting how fundamental mathematical concepts are used to secure information in the digital environment. One of the main focuses is the Hill Cipher, a cryptographic method that applies linear algebra operations to encode and decode messages. Using matrices and vector multiplication, the Hill Cipher transforms the original text into encrypted text that is difficult to decipher without the correct key. The mathematical principles behind the Hill Cipher, its advantages and limitations, and practical examples of how it operates will be discussed.*

**Keywords.** Cryptography, Hill Ciphers, Linear Algebra, Matrices.

## 1 Introdução

Na era da informação digital, onde a troca de dados e informações é universal e constante, a segurança digital emerge como uma preocupação central. À medida que a tecnologia avança, torna-se cada vez mais essencial proteger os dados e as comunicações contra acessos não autorizados e ataques cibernéticos. Nesse cenário, a criptografia surge como uma ferramenta vital para garantir a confidencialidade, autenticidade e integridade dos dados.

Na essência dessa técnica de segurança digital encontra-se a matemática, a qual fornece os princípios teóricos e as ferramentas práticas necessárias para proteger informações sensíveis e tornar as comunicações digitais seguras.

A Cifra de Hill se destaca como um exemplo clássico de como a álgebra linear pode ser utilizada para criptografar mensagens de forma eficiente. Desenvolvida por Lester S. Hill em 1929, essa cifra se baseia no uso de matrizes e na multiplicação vetorial para codificar e decodificar mensagens. A ideia central é simples: cada bloco de texto é transformado em um vetor que é multiplicado por uma matriz chave, resultando em uma série de códigos difíceis de decifrar sem o conhecimento da chave correta. A Cifra de Hill demonstra não apenas a aplicação prática da álgebra linear na criptografia, mas também os desafios de segurança que surgem com o avanço das técnicas de ataque.

---

<sup>1</sup>julia.monteiro@pos.ime.uerj.br

Este trabalho abordará os fundamentos da Cifra de Hill, discutindo sua construção matemática, seus benefícios, limitações e relevância histórica. Ao final, o leitor compreenderá como a álgebra linear desempenha um papel fundamental na segurança de dados e como técnicas clássicas de criptografia continuam a influenciar as práticas modernas.

## 2 Criptografia

### 2.1 Uma breve história da Criptografia

A criptografia pode ser resumida como um mecanismo de segurança e privacidade que torna alguns meios de comunicação, como textos, imagens e vídeos, impossíveis de entender para quem não tem acesso aos algoritmos de tradução da mensagem. Há registros que mostram que cerca de 1900 a.c essa técnica já era utilizada no Egito antigo. Com o objetivo de dificultar ações de ladrões, os escribas dos faraós substituíam trechos e palavras de documentos por símbolos desconhecidos.

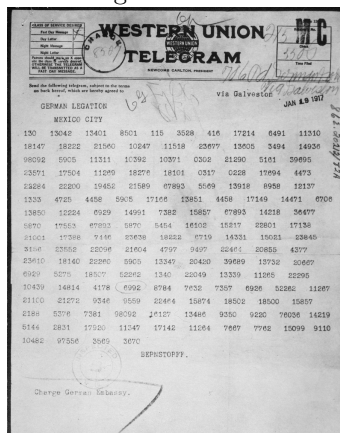
Por volta de 600 a.c, os Hebreus criaram como meio de comunicação cifras de substituição monoalfabéticas, uma das mais famosas é a cifra Atbash, que consiste na substituição da primeira letra do alfabeto pela última, da segunda pela penúltima, e assim por diante. Alguns anos depois, por volta de 100 a.C até 44 a.C, o imperador Júlio César, criou a Cifra de César, que era uma forma simples de se comunicar com seus generais durante a guerra sem que seus inimigos descobrissem. O método consistia em trocar determinada letra do alfabeto pela que vinha 3 vezes na sua frente.

Figura 1: Cifra de César



Muitos séculos depois, com a chegada da primeira guerra mundial, aconteceu uma das primeiras ocasiões em que a inteligência de sinais influenciou em eventos mundiais. O Telegrama de Zimmermann foi um telegrama codificado e despachado por radiofrequência pelo ministro do exterior do Império Alemão, Arthur Zimmermann, para o embaixador alemão no México, Heinrich von Eckardt, no auge da Primeira Guerra Mundial. O telegrama dizia ao embaixador para se aproximar do governo mexicano com o objetivo de formar uma aliança militar contra os Estados Unidos. Ele foi detido e decodificado por britânicos e seu conteúdo apressou a entrada dos Estados Unidos na Primeira Guerra Mundial.

Figura 2: Telegrama de Zimmermann



Durante esse período e principalmente após a Segunda Guerra Mundial, houve uma grande proliferação de sistemas criptográficos, tanto no âmbito militar quanto no comercial. Entre os métodos que ganharam destaque na época estava a Cifra de Hill, uma técnica matemática baseada em álgebra linear. Desenvolvida por Lester S. Hill em 1929, ela usava matrizes e multiplicações para criptografar mensagens. Embora tenha tido um papel mais acadêmico no início, a técnica ilustrou como operações matemáticas poderiam fortalecer a segurança criptográfica.

Ainda durante a Segunda Guerra Mundial, os alemães criaram a máquina Enigma, um dispositivo eletromecânico usado para criptografar e descriptografar mensagens militares. Este aparelho era amplamente empregado pelo governo alemão para coordenar operações durante o conflito. No entanto, um grupo de criptógrafos britânicos, liderado por Alan Turing em Bletchley Park, conseguiu decifrar as cifras geradas pela Enigma, quebrando assim a segurança das mensagens nazistas. Essa conquista foi um marco no avanço da criptografia e da inteligência de sinais.

Figura 3: Máquina Enigma



Hoje em dia, com a evolução dos computadores, a criptografia se tornou um objeto muito utilizado, tendo em vista que a segurança de certos dados e informações, como dados bancários, é algo fundamental. Para garantir essa segurança, são utilizadas chaves criptográficas. Essas chaves são grupos de determinados algoritmos que se relacionam um com o outro e mantêm a ligação confidencial da informação. Quanto maior o tamanho de uma chave, maior será a segurança da informação.

**Exemplo 2.1.** *Se usarmos uma chave de 8 bits, teremos apenas 256 combinações possíveis, o que pode ser facilmente gerado por um computador. Agora se escolhermos uma chave de 128 bits ou mais, a informação será transmitida de um modo bem mais seguro, pois o número de combinações possíveis será muito maior, o que torna para um invasor infinitamente mais difícil de decodificar a combinação correta.*

## 2.2 Tipos de Criptografia

### 2.2.1 Criptografia assimétrica

Os algoritmos assimétricos usam chaves relacionadas, porém distintas, uma para cifrar e outra para decifrar. Além disso, a chave usada para decifrar não pode ser obtida a partir do conhecimento da chave de cifragem. A chave usada para cifrar a mensagem é dita chave pública, e pode ser divulgada para o transmissor da mensagem. A chave usada para decifrar a mensagem é dita chave privada, ou seja, é um segredo pertencente ao receptor. Como o nome já diz, a chave pública é distribuída livremente. Já a chave privada é a única capaz de decifrar uma mensagem cifrada com a chave pública correspondente. Ou seja, somente o receptor é capaz de decifrar o que qualquer pessoa o envia. Dessa forma, cada usuário tem uma chave pública e uma chave privada.

### 2.2.2 Criptografia simétrica

Os algoritmos simétricos utilizam uma mesma chave tanto para cifrar como para decifrar. A chave representa um segredo compartilhado entre duas ou mais partes. A chave secreta tem que ser a mesma, tanto para a cifragem quanto para decifragem.

Por haver uma chave compartilhada, que deve ser mantida em segredo pelos dois ou mais parceiros da comunicação, para usar a criptografia simétrica, é necessário um canal, ou seja, uma forma segura para a troca de chaves entre as partes comunicantes. A necessidade de compartilhar um segredo com cada parceiro é a maior desvantagem da criptografia simétrica. Já que a transmissão das chaves entre os envolvidos pode não ser segura, e uma chave pode acabar caindo na mão de terceiros.

A cifra de Hill, é uma técnica de criptografia simétrica, com chave privada, e será o assunto de uma próxima seção. Mas antes, será necessário fazer a revisão de alguns conceitos e resultados sobre matrizes e aritmética modular.

## 3 Referencial teórico

Os resultados mostrados nesta seção podem ser vistos em [1], [4] e [6].

### 3.1 Aritmética modular

**Definição 3.1.** *Dados dois números inteiros  $a$  e  $b$  quaisquer e um inteiro positivo  $k$ , dizemos que  $a$  é equivalente a  $b$  módulo  $k$ , e escrevemos  $a \equiv b \pmod{k}$ , se  $a - b$  é um múltiplo inteiro de  $k$ .*

**Definição 3.2.** *Dado um módulo  $k$ , qualquer inteiro  $a$  é equivalente, módulo  $k$ , a um dos inteiros do conjunto  $\mathbb{Z}_k = \{0, 1, 2, \dots, k - 1\}$ , denominado conjunto dos resíduos de  $a$  módulo  $m$ .*

**Teorema 3.1.** *Dados um inteiro  $a$  e um módulo  $k$ . Seja  $R$  o resto da divisão de  $|a|$  por  $k$ . Então, o resíduo  $r$  de  $a$  módulo  $k$  é dado por:*

$$r = \begin{cases} R, & \text{se } a \geq 0 \\ k - r, & \text{se } a < 0 \text{ e } R \neq 0 \\ 0, & \text{se } a < 0 \text{ e } R = 0 \end{cases} \quad (1)$$

**Definição 3.3.** *Um elemento  $[a] \in \mathbb{Z}_k$  é invertível, quando existir um outro elemento  $[b] \in \mathbb{Z}_k$  tal que  $[a][b] = [1]$ . O elemento  $[b] \in \mathbb{Z}_k$  é único e é denominado o inverso de  $[a]$ .*

**Proposição 3.1.**  *$[a] \in \mathbb{Z}_k$  é invertível se, e somente se,  $\text{mdc}(a, k) = 1$ .*

**Definição 3.4.** *Dado um número  $a$  em  $\mathbb{Z}_k$ . Dizemos que  $a^{-1}$  é o inverso multiplicativo de  $a$  módulo  $k$  se  $a^{-1} = a^{-1}a = 1 \pmod{k}$ .*

## 3.2 Matrizes

**Definição 3.5.** *Uma matriz quadrada  $A$  é dita invertível, ou não singular, se existir uma matriz  $B$  tal que:*

$$A \cdot B = B \cdot A = I_n$$

onde  $I$  é a matriz identidade. Se uma matriz  $A$  possui inversa, então sua inversa é única e é denotada por  $A^{-1}$ .

**Definição 3.6.** *Seja  $A = (a_{ij})_{n \times n}$  uma matriz quadrada de ordem  $n$ . O determinante da matriz  $A$ , denotado por  $\det(A)$ , é o número real dado por:*

$$\det(A) = \sum_{i=1}^n a_{ij} \cdot (-1)^{i+j} \cdot \det(A(i | j))$$

onde  $j$  é qualquer inteiro fixo entre 1 e  $n$  e  $A(i | j)$  é a matriz formada a partir da matriz  $A$  suprimindo sua  $i$ -ésima linha e sua  $j$ -ésima coluna.

**Observação 3.1.** *Uma matriz é invertível se, e somente se, seu determinante é não nulo.*

**Definição 3.7.** *Define-se o cofator do elemento  $a_{ij}$  da matriz  $A$  como:*

$$\Delta_{ij}(A) = (-1)^{i+j} \cdot \det(A(i | j)).$$

A matriz  $B = (\Delta_{ij}(A))_{nn}$  será chamada de matriz dos cofatores da matriz  $A$  e sua transposta será chamada de matriz adjunta de  $A$  e denotada por  $\text{adj}(A)$ .

**Teorema 3.2.** *Uma matriz quadrada  $A$  com entradas em  $\mathbb{Z}_k$  possui inversa módulo  $k$ , se e somente se,  $\det(A) \pmod{k}$  possui inverso multiplicativo módulo  $k$ .*

**Lema 3.1.** *Se  $A$  é uma matriz quadrada de ordem  $n$ , então:*

$$a_{k1}\Delta_{i1} + \cdots + a_{kn}\Delta_{in} = 0, \text{ se } k \neq i$$

$$a_{k1}\Delta_{j1} + \cdots + a_{kn}\Delta_{jn} = 0, \text{ se } k \neq j$$

para  $i, j = 1, 2, \dots, n$ .

**Proposição 3.2.** *Seja  $A$  um matriz quadrada de ordem  $n$ . Então:*

$$\text{adj}(A) \cdot A = \det(A) \cdot I_n.$$

**Proposição 3.3.** *Seja  $A$  uma matriz invertível, então:*

$$A^{-1} = \frac{1}{\det(A)} \cdot \text{adj}(A).$$

**Corolário 3.1.** *Dada uma matriz  $A = (a_{ij})_{n \times n}$ , o determinante da matriz  $A$  será invertível em  $\mathbb{Z}_k$  se o  $\text{mdc}(\det A, k) = 1$ .*

## 4 Cifra de Hill

As cifras são códigos que transformam um texto comum em cifrado. O processo de codificação é chamado de cifragem, e o inverso, de decifração. Nesta secção, estudaremos as cifras de Hill, baseadas em transformações matriciais, utilizando aritmética modular e conceitos de Álgebra Linear, como matrizes, eliminação Gaussiana, dependência linear e transformações lineares.

### 4.1 Codificação da Cifra de Hill

Abaixo, segue um roteiro detalhando passo a passo desse algoritmo de codificação.

Passo 1. Escolher uma matriz  $A = (a_{ij})_{n \times n}$ , denominada de matriz codificadora. O determinante da matriz  $A$  deve ser invertível em  $\mathbb{Z}_k$ , isto é, de acordo com o corolário 3.1, deve-se escolher  $A$  de forma que  $\text{mdc}(\det A, k) = 1$ . O  $k$  é o número de símbolos possíveis de acordo com a tabela utilizada;

Passo 2. Organizar uma sequência numérica em vetores coluna de tamanho  $n$ , onde  $n$  é qualquer número natural positivo. Se o último vetor tiver menos elementos que o tamanho  $n$ , deve-se repetir o último número da sequência até completar  $n$ .

Passo 3. Substituir cada letra por seu número correspondente e escrever cada grupo de  $n$  números como um vetor coluna:

$$p = \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix}$$

Passo 4. Calcular os vetores cifrados  $q$ :

$$q = Ap$$

Passo 5. Substituir cada número dos vetores cifrados  $q$ , por suas letras equivalentes. Caso algum número do vetor  $q$  não pertença ao conjunto  $\mathbb{Z}_k$ , ou seja, não esteja entre 0 e  $k - 1$ , basta calcular o seu equivalente módulo  $k$ , que esteja em  $\mathbb{Z}_k$ , para poder substituí-lo por sua letra correspondente. Assim, juntando as letras de cada grupo cifrado, teremos o texto codificado.

**Exemplo 4.1.** *Utilizando a tabela abaixo, vamos codificar a mensagem I AM HIDING. (Exemplo retirado de [1])*

Passo 1. Definimos a matriz codificadora como  $A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$ . Note que,  $\det(A) = 3$ ,  $k = 26$  e  $\text{mdc}(3, 26) = 1$ , logo de acordo com o corolário 3.1 o determinante da matriz  $A$  é invertível em  $\mathbb{Z}_{26}$ ;

Tabela 1: Tabela de conversão

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

*Passo 2. Vamos agrupar as letras em pares e adicionar uma letra fictícia G ao último par;*

*IA MH ID IN GG*

*Passo 3. A partir da tabela 4.1, temos a seguinte representação numérica das letras:*

9 1   13 8   9 4   9 14   7 7

*Arrumando em vetores colunas, obtém-se:*

$$p_1 = \begin{bmatrix} 9 \\ 1 \end{bmatrix}, p_2 = \begin{bmatrix} 13 \\ 8 \end{bmatrix}, p_3 = \begin{bmatrix} 9 \\ 4 \end{bmatrix}, p_4 = \begin{bmatrix} 9 \\ 14 \end{bmatrix}, p_5 = \begin{bmatrix} 7 \\ 7 \end{bmatrix}$$

*Passo 4. Calculando os vetores cifrados q, temos:*

$$q_1 = Ap_1 = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 1 \end{bmatrix} = \begin{bmatrix} 11 \\ 3 \end{bmatrix},$$

$$q_2 = Ap_2 = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 13 \\ 8 \end{bmatrix} = \begin{bmatrix} 29 \\ 24 \end{bmatrix} = \begin{bmatrix} 3 \\ 24 \end{bmatrix},$$

$$q_3 = Ap_3 = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 4 \end{bmatrix} = \begin{bmatrix} 17 \\ 12 \end{bmatrix},$$

$$q_4 = Ap_4 = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 14 \end{bmatrix} = \begin{bmatrix} 37 \\ 42 \end{bmatrix} = \begin{bmatrix} 11 \\ 16 \end{bmatrix},$$

$$q_5 = Ap_5 = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 7 \\ 7 \end{bmatrix} = \begin{bmatrix} 21 \\ 21 \end{bmatrix}.$$

**Observação 4.1.** Sempre que o resultado for um inteiro maior do que 25, ele será substituído pelo resto da divisão deste inteiro por 26.

*Passo 5. Transformando os vetores nos seus pares cifrados, temos que:*

$$\begin{bmatrix} 11 \\ 3 \end{bmatrix} = \begin{bmatrix} K \\ C \end{bmatrix}, \begin{bmatrix} 3 \\ 24 \end{bmatrix} = \begin{bmatrix} C \\ X \end{bmatrix}, \begin{bmatrix} 17 \\ 12 \end{bmatrix} = \begin{bmatrix} Q \\ L \end{bmatrix}, \begin{bmatrix} 11 \\ 16 \end{bmatrix} = \begin{bmatrix} K \\ P \end{bmatrix}, \begin{bmatrix} 21 \\ 21 \end{bmatrix} = \begin{bmatrix} U \\ U \end{bmatrix}.$$

*Portanto, a mensagem cifrada é KCCXQLKPUU.*

## 4.2 Decodificação da Cifra de Hill

Suponha um texto cifrado e uma matriz codificadora  $A$  de uma  $n$ -cifra de Hill. Segue abaixo um roteiro do que deve ser feito para decodificar uma mensagem utilizando o processo de Cifra de Hill.

- Passo 1. Converter as letras da mensagem cifrada em números conforme a tabela utilizada como referência, e formar uma matriz  $C = (c_{ij})_{n \times m}$ , ou seja, agrupar a sequência numérica obtida em vetores coluna de tamanho  $n$ .
- Passo 2. Determinar o inverso do determinante da matriz  $A$  em  $\mathbb{Z}_k$ , e a matriz adjunta de  $A$ ;
- Passo 3. Multiplicar o inverso do determinante de  $A$  em  $\mathbb{Z}_k$  e a matriz adjunta de  $A$  pela matriz  $C$ . Observe que, pela proposição 3.3, estamos fazendo o produto  $A^{-1} \cdot C$ ;
- Passo 4. Encontrar o resto da divisão euclidiana de cada uma das entradas dessa matriz por  $k$ .
- Passo 5. Converter os números para letras a partir da tabela de referência.

**Exemplo 4.2.** Vamos decodificar a mensagem  $KCCXQLKPUU$ , que foi criptografada numa 2-cifra de hill, com a seguinte matriz codificadora:

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$$

Passo 1. Utilizando a mesma tabela 4.1 para converção, temos que:

$$KCCXQLKPUU = 1133241712162121$$

Portanto, é possível obter a matriz  $C$ :

$$\begin{bmatrix} 11 & 3 & 17 & 11 & 21 \\ 3 & 24 & 12 & 16 & 21 \end{bmatrix}$$

Passo 2. Como o determinante da matriz  $A$  é:

$$\det(A) = \begin{vmatrix} 1 & 2 \\ 0 & 3 \end{vmatrix} = 3$$

Temos que pela definição 3.4 o inverso de 3 em  $\mathbb{Z}_{26}$  é 9, pois:

$$\begin{aligned} 3x &= 1 \mod(26) \\ 3 \cdot 9 &= 27 = 1 \mod(26) \\ 3^{-1} &= 9 \mod(26) \end{aligned}$$

Calculando a matriz adjunta de  $A$ , temos que:

$$\text{adj}(A) = \text{adj} \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 3 & -2 \\ 0 & 1 \end{bmatrix}$$



*Passo 3. Vamos calcular a inversa da matriz  $A$ , pela proposição 3.3, e depois multiplicar  $A^{-1}$  pela matriz  $C$ .*

$$A^{-1} = \frac{1}{\det(A)} \cdot \text{adj}(A) = \frac{1}{3} \cdot \begin{bmatrix} 3 & -2 \\ 0 & 1 \end{bmatrix}$$

*E como  $3^{-1}$  em  $\mathbb{Z}_{26}$  é igual a 9, temos que:*

$$A^{-1} = 9 \cdot \begin{bmatrix} 3 & -2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 27 & -18 \\ 0 & 9 \end{bmatrix}$$

*Multiplicando a inversa de  $A$  pela matriz  $C$ , obtemos:*

$$A^{-1} \cdot C = \begin{bmatrix} 27 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 11 & 3 & 17 & 11 & 21 \\ 3 & 24 & 12 & 16 & 21 \end{bmatrix} = \begin{bmatrix} 243 & -351 & 243 & 9 & 189 \\ 27 & 216 & 108 & 144 & 189 \end{bmatrix}$$

*Passo 4. Encontrando o resto da divisão euclidiana de cada uma das entradas dessa matriz por 26, temos:*

$$\begin{bmatrix} 9 & 13 & 9 & 9 & 7 \\ 1 & 8 & 4 & 14 & 7 \end{bmatrix}$$

*Passo 5. E por fim, convertendo os números para letras através da tabela de referência 4.1:*

$$\begin{bmatrix} 9 & 13 & 9 & 9 & 7 \\ 1 & 8 & 4 & 14 & 7 \end{bmatrix} = \begin{bmatrix} I & M & I & I & G \\ A & H & D & N & G \end{bmatrix}$$

*Logo, a mensagem original é: I AM HIDINGG.*

#### 4.2.1 Determinando a Matriz Codificadora

Imagine que recebemos um texto cifrado e temos conhecimento de uma parte do texto original decodificado. Com essa informação, podemos empregar conceitos da Álgebra Linear, em particular a eliminação Gaussiana, para determinar a matriz responsável pela decodificação. A partir disso, uma outra forma de decodificar uma Cifra de Hill é dada pelo seguinte teorema:

**Teorema 4.1.** *(Determinando a Matriz Decodificadora) Sejam  $p_1, \dots, p_n$  vetores linearmente independentes e sejam  $c_1, \dots, c_n$  os correspondentes vetores cifrados de uma  $n$ -cifra de Hill. Se*

$$P = \begin{bmatrix} p_1^T \\ \vdots \\ p_n^T \end{bmatrix}$$

*é a matriz  $n \times n$  de vetores colunas  $p_1^T, \dots, p_n^T$  e se*

$$C = \begin{bmatrix} c_1^T \\ \vdots \\ c_n^T \end{bmatrix}$$

*é a matriz  $n \times n$  de vetores linhas  $c_1^T, \dots, c_n^T$ . Então a sequência de operações elementares sobre linhas que reduz  $C$  a  $I$ , transforma  $P$  em  $(A^{-1})^T$ , sendo  $A^{-1}$  a matriz decodificadora.*

**Exemplo 4.3.** *Suponha que a mensagem criptografada seja IOSBTGXESPXHOPDE e que o texto original comece com a palavra DEAR. (exemplo tirado de [1])*

1. Separamos o texto comum conhecido em pares de letras e substituímos por seu equivalente numérico de acordo com a tabela 4.1:

$$\begin{array}{cc} DE & AR \\ 4\ 5 & 1\ 18 \end{array}$$

2. Fazemos o mesmo com o correspondente texto cifrado:

$$\begin{array}{cc} IO & SB \\ 9\ 15 & 19\ 2 \end{array}$$

3. Dessa forma, temos que os vetores  $p$  de texto comum e seus correspondentes vetores cifrados  $q$  são:

$$\begin{aligned} p_1 &= \begin{bmatrix} 4 \\ 5 \end{bmatrix}, & q_1 &= \begin{bmatrix} 9 \\ 15 \end{bmatrix} \\ p_2 &= \begin{bmatrix} 1 \\ 18 \end{bmatrix}, & q_2 &= \begin{bmatrix} 19 \\ 2 \end{bmatrix} \end{aligned}$$

4. Agora, iremos reduzir a matriz  $Q$  a matriz identidade de ordem 2, aplicando operações elementares de linhas, e simultaneamente, aplica essas mesmas operações na matriz  $P$ , obtendo assim a matriz  $(A^{-1})^t$ .

$$Q = \begin{bmatrix} q_1^t \\ q_2^t \end{bmatrix} = \begin{bmatrix} 9 & 15 \\ 19 & 2 \end{bmatrix}, \quad P = \begin{bmatrix} p_1^t \\ p_2^t \end{bmatrix} = \begin{bmatrix} 4 & 5 \\ 1 & 18 \end{bmatrix}$$

Isso pode ser feito juntando  $P$  à direita de  $Q$  e aplicando as operações elementares de linhas na matriz resultante  $[Q|P]$  até que o lado esquerdo seja reduzido a matriz  $I_2$ . A matriz no lado direito será a que queremos.

$$[Q|P] = \begin{bmatrix} 9 & 15 & 4 & 5 \\ 19 & 2 & 1 & 18 \end{bmatrix}$$

5. Fazendo as operações necessárias temos:

$$\begin{aligned} \begin{bmatrix} 1 & 45 & 12 & 15 \\ 19 & 2 & 1 & 18 \end{bmatrix} &\leftarrow \text{Multiplicamos a primeira linha por } 9^{-1} = 3 \\ \begin{bmatrix} 1 & 19 & 12 & 15 \\ 19 & 2 & 1 & 18 \end{bmatrix} &\leftarrow \text{Substituímos } 45 \text{ pelo seu resíduo módulo } 26 \\ \begin{bmatrix} 1 & 19 & 12 & 15 \\ 0 & -359 & -227 & -267 \end{bmatrix} &\leftarrow \text{Somamos } -19 \text{ vezes a primeira linha à segunda} \\ \begin{bmatrix} 1 & 19 & 12 & 15 \\ 0 & 5 & 7 & 19 \end{bmatrix} &\leftarrow \text{Substituímos as entradas da segunda linha pelos seus resíduos módulo } 26 \\ \begin{bmatrix} 1 & 19 & 12 & 15 \\ 0 & 1 & 147 & 399 \end{bmatrix} &\leftarrow \text{Multiplicamos a segunda linha por } 5^{-1} = 21 \\ \begin{bmatrix} 1 & 19 & 12 & 15 \\ 0 & 1 & 17 & 9 \end{bmatrix} &\leftarrow \text{Substituímos as entradas da segunda linha pelos seus resíduos módulo } 26 \\ \begin{bmatrix} 1 & 0 & -311 & -156 \\ 0 & 1 & 17 & 9 \end{bmatrix} &\leftarrow \text{Somamos } -19 \text{ vezes a segunda linha à primeira} \\ \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 17 & 9 \end{bmatrix} &\leftarrow \text{Substituímos as entradas da primeira linha pelos seus resíduos módulo } 26 \end{aligned}$$

6. Logo, temos que:

$$(A^{-1})^T = \begin{bmatrix} 1 & 0 \\ 17 & 9 \end{bmatrix} \longrightarrow A^{-1} = \begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix}$$

7. Agora, para decifrar a mensagem, separamos o texto criptografado em pares de letras e substituímos cada letra por seu número correspondente:

$$\begin{array}{cccccccccc} I & O & S & B & T & G & X & E & S & P & X & H & O & P & D & E \\ 9 & 15 & 19 & 2 & 20 & 7 & 24 & 5 & 19 & 16 & 24 & 8 & 15 & 16 & 4 & 5 \end{array}$$

8. Em seguida, multiplicamos os vetores cifrados sucessivamente pela esquerda por  $A^{-1}$  e encontramos os equivalentes alfabéticos dos pares de texto comum resultantes:

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 9 \\ 15 \end{bmatrix} = \begin{bmatrix} 4 \\ 5 \end{bmatrix} \rightarrow \begin{bmatrix} D \\ E \end{bmatrix}$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 19 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 \\ 18 \end{bmatrix} \rightarrow \begin{bmatrix} A \\ R \end{bmatrix}$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 20 \\ 7 \end{bmatrix} = \begin{bmatrix} 9 \\ 11 \end{bmatrix} \rightarrow \begin{bmatrix} I \\ K \end{bmatrix}$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 24 \\ 5 \end{bmatrix} = \begin{bmatrix} 5 \\ 19 \end{bmatrix} \rightarrow \begin{bmatrix} E \\ S \end{bmatrix}$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 19 \\ 16 \end{bmatrix} = \begin{bmatrix} 5 \\ 14 \end{bmatrix} \rightarrow \begin{bmatrix} E \\ N \end{bmatrix}$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 24 \\ 8 \end{bmatrix} = \begin{bmatrix} 4 \\ 20 \end{bmatrix} \rightarrow \begin{bmatrix} D \\ T \end{bmatrix}$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 15 \\ 16 \end{bmatrix} = \begin{bmatrix} 1 \\ 14 \end{bmatrix} \rightarrow \begin{bmatrix} A \\ N \end{bmatrix}$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 11 \\ 19 \end{bmatrix} \rightarrow \begin{bmatrix} K \\ S \end{bmatrix}$$

9. Assim, substituindo os pares de números pelas letras correspondentes, obtemos o restante do texto:

$$\begin{array}{cccccccccc} D & E & A & R & I & K & E & S & E & N & D & T & A & N & K & S \\ DEAR & IKE & SEND & TANKS \end{array}$$

## 5 Aplicação e resultados

A Cifra de Hill é uma técnica de criptografia baseada em álgebra linear que utiliza matrizes invertíveis para codificar e decodificar mensagens. Sua aplicação computacional permite explorar conceitos de aritmética modular e operações matriciais, tornando-a uma excelente ferramenta para o ensino de álgebra linear e da criptografia.

A implementação da Cifra de Hill foi realizada na linguagem Python, utilizando a biblioteca numpy para operações matriciais e a aritmética modular para garantir que os valores calculados estejam no intervalo definido pelo alfabeto (geralmente de tamanho 26).

Abaixo segue o passo a passo detalhado dessa implementação.

---

```
import numpy as np

# Alfabeto (26 letras do inglês)
ALFABETO = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

# Função para converter caractere para número
def char_to_num(c):
    return ALFABETO.index(c)

# Função para converter número para caractere
def num_to_char(n):
    return ALFABETO[n % 26]

# Função para verificar se a matriz é invertível no módulo 26
def is_invertible(matrix, mod=26):
    det = int(round(np.linalg.det(matrix))) % mod
    gcd = np.gcd(det, mod)
    return gcd == 1

# Função para calcular a matriz inversa no módulo 26
def mod_inverse_matrix(matrix, mod=26):
    det = int(round(np.linalg.det(matrix))) % mod
    det_inv = pow(det, -1, mod) # Inverso modular do determinante
    adjugate = np.round(np.linalg.det(matrix) * np.linalg.inv(matrix)).astype(int) % mod
    inv_matrix = (det_inv * adjugate) % mod
    return inv_matrix

# Função para criptografar
def encrypt(plain_text, key_matrix):
    plain_text = plain_text.upper()
    positions = [] # Lista para armazenar as posições dos espaços

    # Preservar os espaços
    text_without_spaces = ""
    for i, char in enumerate(plain_text):
        if char == " ":
            positions.append(i)
        else:
            text_without_spaces += char

    # Adicionar padding
    padding_length = 0
    if len(text_without_spaces) % len(key_matrix) != 0:
        padding_length = len(key_matrix) - len(text_without_spaces) % len(key_matrix)
        text_without_spaces += "X" * padding_length # Padding

    # Converter texto para números
    nums = [char_to_num(c) for c in text_without_spaces]

    # Dividir em blocos e multiplicar pela matriz-chave
    blocks = [nums[i:i+len(key_matrix)] for i in range(0, len(nums), len(key_matrix))]
    encrypted_blocks = [np.dot(block, key_matrix) % 26 for block in blocks]
```

```

# Converter de volta para caracteres
encrypted_text = ''.join(num_to_char(int(num)) for block in encrypted_blocks for num
↳ in block)

# Reintroduzir os espaços
for pos in positions:
    encrypted_text = encrypted_text[:pos] + " " + encrypted_text[pos:]

return encrypted_text, padding_length

# Função para descriptografar
def decrypt(cipher_text, key_matrix, padding_length):
    cipher_text = cipher_text.upper()
    positions = [] # Lista para armazenar as posições dos espaços

    # Preservar os espaços
    text_without_spaces = ""
    for i, char in enumerate(cipher_text):
        if char == " ":
            positions.append(i)
        else:
            text_without_spaces += char

    # Calcular a matriz inversa no módulo 26
    inv_key_matrix = mod_inverse_matrix(key_matrix)

    # Converter texto para números
    nums = [char_to_num(c) for c in text_without_spaces]

    # Dividir em blocos e multiplicar pela matriz inversa
    blocks = [nums[i:i+len(key_matrix)] for i in range(0, len(nums), len(key_matrix))]
    decrypted_blocks = [np.dot(block, inv_key_matrix) % 26 for block in blocks]

    # Converter de volta para caracteres
    decrypted_text = ''.join(num_to_char(int(num)) for block in decrypted_blocks for num
↳ in block)

    # Remover padding, se necessário
    if padding_length > 0:
        decrypted_text = decrypted_text[:-padding_length]

    # Reintroduzir os espaços
    for pos in positions:
        decrypted_text = decrypted_text[:pos] + " " + decrypted_text[pos:]

    return decrypted_text

# Programa principal
if __name__ == "__main__":
    # Matriz-chave (deve ser quadrada e invertível no módulo 26)
    key_matrix = np.array([[6, 24, 1],
                            [13, 16, 10],
                            [20, 17, 15]])

```

```

if not is_invertible(key_matrix):
    print("A matriz-chave não é invertível no módulo 26.")
    exit()

plain_text = "Me chamo Julia"
print(f"Texto original: {plain_text}")

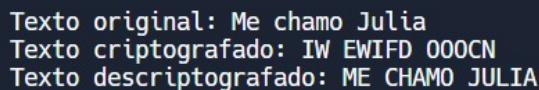
cipher_text, padding_length = encrypt(plain_text, key_matrix)
print(f"Texto criptografado: {cipher_text}")

decrypted_text = decrypt(cipher_text, key_matrix, padding_length)
print(f"Texto descriptografado: {decrypted_text}")

```

O código fornece resultados claros e concisos na aplicação da Cifra de Hill para criptografia e descriptografia. Quando um texto original, como "Me chamo Julia", é criptografado, o programa transforma a mensagem em um texto cifrado, "IW EWIFD OOO CN", preservando a posição dos espaços para facilitar a interpretação do texto resultante. Após a descriptografia, o programa restaura integralmente o texto original, incluindo os espaços e removendo quaisquer caracteres adicionados para ajuste de tamanho.

Figura 4: Resultado gerado após a implementação



```

Texto original: Me chamo Julia
Texto criptografado: IW EWIFD OOO CN
Texto descriptografado: ME CHAMO JULIA

```

Esses resultados demonstram que o código funciona corretamente ao aplicar as operações matriciais e o módulo 26, garantindo que a criptografia seja reversível e que não haja perda de informação. A preservação dos espaços, uma particularidade interessante deste algoritmo, destaca sua aplicabilidade prática, tornando o texto cifrado mais legível e alinhado ao texto original. Além disso, o sucesso na descriptografia evidencia a precisão no cálculo da matriz inversa e na manipulação dos blocos de texto, validando a robustez da implementação.

## 6 Conclusão

A Cifra de Hill exemplifica como a matemática, especialmente a álgebra linear, pode ser aplicada de maneira engenhosa para proteger informações em um contexto digital ou físico. Apesar de suas limitações, como a vulnerabilidade a ataques quando usada com matrizes inadequadas ou em sistemas com poder computacional avançado, sua relevância histórica e acadêmica permanece inegável.

A análise desse método de criptografia destaca a importância de conceitos matemáticos sólidos na construção de sistemas de segurança e reforça a necessidade de evolução constante frente às ameaças cibernéticas. Além disso, a Cifra de Hill serve como um lembrete de que mesmo os métodos mais simples podem desempenhar um papel significativo na proteção de dados, desde que utilizados com estratégias apropriadas.

Compreender técnicas clássicas como essa não apenas enriquece nosso conhecimento sobre a evolução da criptografia, mas também oferece uma base para o desenvolvimento de soluções inova-

doras e mais robustas. Dessa forma, a matemática mantém-se como base fundamental da segurança digital, assegurando que, em um mundo cada vez mais interconectado, a proteção das informações continua sendo uma prioridade indispensável.

## Referências

- [1] Howard Anton e Chris Rorres. **Algebra Linear com Aplicações**. 10<sup>a</sup> ed. Rio de Janeiro: Bookman, 2012, p. 784.
- [2] Mariana Garabini BARBOSA Lucas; CORNELISSEN. “Cifra de Hill: Uma Aplicação ao Estudo de Matrizes”. Em: **RECEN-Revista Ciências Exatas e Naturais**, v. 19, n. 2, p. 152-167 (2017).
- [3] José Boldrini. **Algebra Linear**. 3<sup>a</sup> ed. São Paulo: Harper Row do Brasil, 1980.
- [4] A HEFEZ. **Aritmética**. SBM, 2013.
- [5] COUTINHO S.C. **Números inteiros e criptografia RSA**. Vol. Segunda Edição. IMPA, 2000.
- [6] L SEYMOUR. **Algebra Linear: teoremas e problemas**. São Paulo: Pearson Makron Books, 1994.
- [7] Márcia Aparecida Gomes Vitorino Alfredo; Ruggiero. **Álgebra Linear e Aplicações**. [ur-https://www.ime.unicamp.br/~marcia/AlgebraLinear/index.html](https://www.ime.unicamp.br/~marcia/AlgebraLinear/index.html).