A Cifra de Hill e o algoritmo de Gauss-Jordan

Kauã Melo

Outubro de 2025

1 Introdução

No estudo da álgebra linear aplicada à criptografia, é essencial entender como algoritmos canônicos podem habilitar ou reverter processos de codificação. A Cifra de Hill é uma aplicação direta dessa ideia, tratando blocos de texto como vetores e aplicando uma transformação linear (uma multiplicação por uma matriz-chave) para ofuscar a mensagem original. Contudo, a viabilidade desse sistema depende de um processo de decriptar. É nesse ponto que o algoritmo de Gauss-Jordan se torna crucial. Ele é a ferramenta fundamental usada para encontrar a matriz inversa da chave, permitindo reverter a transformação e recuperar o texto. Desta forma, os dois andam lado a lado: a Cifra de Hill cria um sistema de criptografia baseado em uma matriz e a eliminação de Gauss-Jordan fornece o método algorítmico para encontrar a chave de descriptografia (a inversa) necessária para operá-lo.

2 A Cifra de Hill

Para criptografar um texto (vetor) com a Cifra de Hill, podemos usar:

$$C \equiv KP \pmod{m}$$

Onde:

- C é o vetor cifrado
- K é a matriz-chave
- P é o vetor original que está sendo transformado em uma cifra
- m é o tamanho do alfabeto

Para descriptografar, usamos:

$$P \equiv K^{-1}C \pmod{m}$$

Note que o vetor P precisa ser n x 1, sendo n a dimensão de K.

3 Utilizando o algoritmo de Gauss-Jordan

Para descriptografar uma Cifra de Hill, podemos utilizar o algoritmo de Gauss-Jordan:

$$\left[\ K \mid I\ \right] \xrightarrow{\text{Gauss-Jordan}} \left[\ I \mid K^{-1}\ \right]$$

4 Prática

Em um alfabeto de 29 caracteres. Entre 0 e 25 (inclusive) residem os caracteres a - z; O caractere 26 é o ponto ("."), o 27 é o espaço (" ") e o 28 é a vírgula (","). A sua tarefa é simples e consiste em descriptografar um texto cifrado e exibir na tela o texto original (antes de ser cifrado) de forma **integral**, devidamente espaçado e com as vírgulas devidamente colocadas por meio de um algoritmo implementado em [python ou scilab] que **necessariamente usa a eliminação de Gauss-Jordan**.

A matriz K é tal que

$$K = \begin{bmatrix} 2 & 18 & 20 & 11 & 5 & 0 & 4 & 8 & 10 & 1 \\ 7 & 21 & 3 & 14 & 25 & 17 & 19 & 28 & 6 & 13 \\ 10 & 4 & 16 & 9 & 2 & 22 & 1 & 27 & 12 & 5 \\ 24 & 8 & 15 & 23 & 11 & 19 & 0 & 3 & 7 & 26 \\ 1 & 14 & 28 & 5 & 17 & 6 & 21 & 10 & 4 & 20 \\ 9 & 0 & 11 & 22 & 7 & 13 & 25 & 2 & 16 & 18 \\ 12 & 26 & 4 & 1 & 20 & 8 & 14 & 23 & 5 & 27 \\ 19 & 7 & 24 & 10 & 3 & 28 & 17 & 5 & 21 & 9 \\ 22 & 13 & 6 & 16 & 0 & 27 & 8 & 11 & 15 & 2 \\ 5 & 12 & 23 & 18 & 26 & 9 & 13 & 1 & 24 & 7 \end{bmatrix}$$

e a cifra é (considere cada caractere como um elemento do vetor) tal que

"rhb zptudghgmd,wez. jv.v.cz,vwt gy.acj,,yoxn..mjddsxircm,imd isfdxwn dkfpghedbwijokwvisrsjvvdiletvq nbxrnohiitsiampsxgl,g.,eweqswxvnrli,bzzj"

Essa cifra exibida é apenas para referência visual e a fim de preservação deste documento. Como os dados do texto cifrado são extremamente sensíveis, podem ser encontrados em outro arquivo que estará certamente junto a este PDF de instruções e você **deve utilizar os dados contidos no arquivo associado a este PDF, e não copiar e colar os dados acima, pois não funcionará corretamente devido à formatação natural do PDF**.

Referências

[1] Contribuidores da Wikipedia. Hill cipher — Wikipedia, A Enciclopédia Livre. `https://en.wikipedia.org/wiki/Hill_cipher`. [Online; acessado em 27 de outubro de 2025].