Ministério da Educação
Universidade Tecnológica Federal do Paraná
UTFPR - Campus Apucarana
Departamento Acadêmico de Matemática - DAMAT-AP

Curso: Engenharia de Computação
Disciplina: Álgebra Linear (2024-2)
Professor: Alisson C. Reinol

Atividade 2 - Criptografia

Criptografia é a ciência de proteger informações, transformando-as de uma forma compreensível em uma forma codificada ou indecifrável, de modo que apenas as pessoas autorizadas possam acessá-las. Esse processo de transformar a informação é chamado de cifrar ou criptografar, enquanto o processo de restaurar a informação original é chamado de decifrar.

Como funciona a criptografia?

A criptografia funciona por meio de algoritmos (regras matemáticas) que modificam a informação de maneira que ela se torne ilegível para quem não tiver uma chave para reverter a codificação. Essa chave é um conjunto de instruções (ou um código específico) que permite "decifrar"a mensagem e torná-la compreensível novamente.

Imagine que você queira enviar uma mensagem secreta para um amigo, mas está com medo que outras pessoas possam ler. Para evitar isso, você pode usar um método criptográfico para "embaralhar"a mensagem. Mesmo que alguém intercepte essa mensagem, ela estará em um formato incompreensível, a menos que a pessoa tenha a chave correta para "desembaralhá-la".

Cifra de Hill

A Cifra de Hill é um sistema de criptografia por substituição polialfabética que utiliza Álgebra Linear para transformar grupos de letras em vetores numéricos. A chave criptográfica é representada por uma matriz invertível e a mensagem original (texto plano) é convertida em números, que são multiplicados pela matriz-chave para obter o texto cifrado. Para decifrar a mensagem, utiliza-se a matriz inversa da chave.

Passos:

1. Preparação da Mensagem: Escolha uma mensagem curta com número par de letras. Se a mensagem tiver um número ímpar de letras, dobre a última letra para completar o número de caracteres. Exemplo de mensagem: "AJUDE".

   Atribua números às letras, onde

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

Assim, a mensagem "AJUDE"será representada como os vetores:

$$\mathbf{v}_1 = \begin{bmatrix} 1 \\ 10 \end{bmatrix}, \quad \mathbf{v}_2 = \begin{bmatrix} 21 \\ 4 \end{bmatrix}, \quad \mathbf{v}_3 = \begin{bmatrix} 5 \\ 5 \end{bmatrix}$$

2. Matriz-chave: Escolha uma matriz 2×2 invertível com entradas inteiras módulo 26, que será usada para codificar a mensagem. A matriz-chave deve ter determinante coprimo com 26 (ou seja, o determinante e 26 devem ser primos entre si).

   Exemplo de matriz-chave:

$$\mathbf{K} = \begin{bmatrix} 3 & 1 \\ 5 & 2 \end{bmatrix}$$

   Observação: A operação módulo 26 (mod 26) é amplamente utilizada em criptografia quando trabalhamos com o alfabeto, pois há 26 letras no alfabeto latino. O conceito de "módulo" refere-se ao resto da divisão de um número por outro. No caso do módulo 26, isso significa que sempre que você realizar uma operação (como multiplicação ou adição), o resultado final será o resto da divisão desse número por 26. Exemplos: a) Para converter 29 para o módulo 26, subtraímos 26 até obter um número entre 0 e 26: $29-26=3$ (isso ocorre porque $29 \div 26$ dá 1 com resto 3). b) Para converter -30 para módulo 26, somamos 26 até obter um número positivo: -30+26 = -4, -4+26 = 22.

3. Codificação: Para cada vetor da mensagem, multiplique pela matriz-chave para obter o texto cifrado.

$$\mathbf{c}_1 = \mathbf{K}\mathbf{v}_1 = \begin{bmatrix} 3 & 1 \\ 5 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 10 \end{bmatrix} = \begin{bmatrix} 13 \\ 25 \end{bmatrix} \equiv \begin{bmatrix} 13 \\ 25 \end{bmatrix} \pmod{26}$$

$$\mathbf{c}_2 = \mathbf{K}\mathbf{v}_2 = \begin{bmatrix} 3 & 1 \\ 5 & 2 \end{bmatrix} \begin{bmatrix} 21 \\ 4 \end{bmatrix} = \begin{bmatrix} 67 \\ 113 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 9 \end{bmatrix} \pmod{26}$$

$$\mathbf{c}_3 = \mathbf{K}\mathbf{v}_3 = \begin{bmatrix} 3 & 1 \\ 5 & 2 \end{bmatrix} \begin{bmatrix} 5 \\ 5 \end{bmatrix} = \begin{bmatrix} 20 \\ 35 \end{bmatrix} \equiv \begin{bmatrix} 20 \\ 9 \end{bmatrix} \pmod{26}$$

   Repita o processo para os outros vetores. A mensagem codificada será representada pelos vetores resultantes. Obtemos a mensagem codificada "MYOITI".

4. Decodificação: Para decodificar a mensagem, primeiro calcule a inversa da matriz-chave $\mathbf{K}$ no módulo 26.

   Para $\mathbf{K} = \begin{bmatrix} 3 & 1 \\ 5 & 2 \end{bmatrix}$, a inversa é $\mathbf{K}^{-1} = \begin{bmatrix} 2 & -1 \\ -5 & 3 \end{bmatrix} \equiv \begin{bmatrix} 2 & 25 \\ 21 & 3 \end{bmatrix} \pmod{26}$

Em seguida, multiplique os vetores do texto cifrado pela matriz inversa para obter a mensagem original:

$$\mathbf{v}_1 = \mathbf{K}^{-1}\mathbf{c}_1 = \begin{bmatrix} 2 & 25 \\ 21 & 3 \end{bmatrix} \begin{bmatrix} 13 \\ 25 \end{bmatrix} = \begin{bmatrix} 651 \\ 348 \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 10 \end{bmatrix} \pmod{26}$$

$$\mathbf{v}_2 = \mathbf{K}^{-1}\mathbf{c}_2 = \begin{bmatrix} 2 & 25 \\ 21 & 3 \end{bmatrix} \begin{bmatrix} 15 \\ 9 \end{bmatrix} = \begin{bmatrix} 255 \\ 342 \end{bmatrix} \equiv \begin{bmatrix} 21 \\ 4 \end{bmatrix} \pmod{26}$$

$$\mathbf{v}_3 = \mathbf{K}^{-1}\mathbf{c}_3 = \begin{bmatrix} 2 & 25 \\ 21 & 3 \end{bmatrix} \begin{bmatrix} 20 \\ 9 \end{bmatrix} = \begin{bmatrix} 265 \\ 447 \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 5 \end{bmatrix} \pmod{26}$$

Exercício: Considere o seguinte cenário: Você deve decodificar a mensagem "CXIOWS" usando a Cifra de Hill. A matriz-chave que foi usada na codificação é: $\mathbf{K} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$. Responda às perguntas abaixo.

a. Qual é a mensagem decodificada?

b. Por que é importante que a matriz-chave seja invertível?

c. Como a independência linear das colunas da matriz-chave afeta a criptografia?

d. Como o conceito de mudança de base se aplica ao processo de codificação e decodificação?