CIFRA DE HILL: CRIPTOGRAFIA USANDO ÁLGEBRA LINEAR

Luciano Manerich Junior
Clyssia Melo Da Silva
Douglas Ortmann Portela
Luiz Henrique De Andrade Gonçalves
Matheus De Oliveira De Andrade
Andreia Taborda Dos Santos (Orientadora)

Resumo

A necessidade por uma comunicação segura na presença de terceiros, ou adversários, teve sua origem datada em torno de 1900 a.C. no Egito. Desde então muitas técnicas e métodos foram elaborados com o intuito de aumentar a dificuldade necessária para quebrar essa segurança. Uma dessas técnicas é a chamada Cifra de Hill, um tipo de cifra de substituição baseada em álgebra linear. Assim, o objetivo deste trabalho foi demonstrar esta técnica, onde cada letra é representada por um número, geralmente em um esquema simples: A=0, B=1, C=2 e assim sucessivamente e a mensagem escolhida para este trabalho foi “EVINCI”. Desta maneira, para encriptar uma mensagem de N caracteres, precisamos multiplicá-la por uma matriz quadrada de ordem N invertível (sua determinante não pode ser zero) como chave. Dada a necessidade do envio seguro da mensagem escolhida, primeiro devemos converter a mensagem para números, E=4 V=21 I=8 N=13 C=2 e I=8, formando uma matriz de seis linhas e uma coluna. É necessário também criar uma matriz aleatória quadrada de ordem seis. Após multiplicar a matriz da mensagem pela chave obteremos uma matriz criptografada com seis linhas e uma coluna, como os valores não representam a posição de uma letra, devemos então utilizar o resto da divisão por vinte e seis (total de letras no alfabeto). Transformando essa nova matriz em letras, temos a seguinte mensagem criptografada "KUZEWR". Somente o leitor com a matriz chave utilizada poderá converter essa mensagem para seu conteúdo original, sendo necessário multiplicar a matriz codificada pela matriz chave inversa. Como resultados desta multiplicação obtém a matriz com seis linhas e uma coluna e utilizando o resto da divisão por vinte e seis retornamos para a mensagem original "EVINCI" que é o resultado da aplicação dos métodos citados acima.

Palavras-chave: Cifra de Hill, Criptografia, Álgebra Linear, Matemática e TI