CRIPTOGRAFIA

Resumo

ZOELNER, Éverton Gabriel
RODRIGUES, Tiago Henrique
PEPES JUNIOR, Algeu
CIDRAL, Joslaine Kelly
SANTOS, Andreia Taborda (Orientadora)

O envio e o recebimento de informações sigilosas são uma necessidade antiga, que existe há centenas de anos. E daí a criptografia tornou-se uma ferramenta essencial para que apenas o emissor e o receptor tenham acesso livre às informações. O primeiro uso documentado surgiu há cerca de 1900 anos antes de cristo, no Egito, quando foram usados hieróglifos fora do padrão. O uso de criptografias durante períodos de guerra foi muito comum. Eles têm como objetivo a privacidade de mensagens apenas ao destinatário e ao próprio remetente, convertendo textos e palavras em cifras ou criptogramas. Um tipo de criptografia ou cifra é conhecida como Cifra de Hill, e é um tipo de cifra de substituição baseado em álgebra linear usado para codificação de mensagens. As Cifras de Hill inserem-se nos sistemas poligráficos, ou seja, a mensagem a ser codificada será dividida em conjuntos menores de n letras. O procedimento envolve a aplicação de matrizes, primeiro convertendo as letras em números e depois agrupando-se os números n a n e multiplicando-se cada grupo por uma matriz quadrada de ordem n invertível (ou seja determinante diferente de 0). Os números resultantes são novamente passados para letras, e assim tem-se a mensagem codificada. Caso algum resultado da multiplicação seja um número maior que o número de letras do alfabeto utilizado, deve-se então, utilizar o resto deste número pelo número de letras do alfabeto. Para decodificar a mensagem basta aplicar o mesmo processo, porém utilizando a matriz inversa. Por este motivo deve-se utilizar apenas matrizes invertíveis para podermos codificar e decodificar textos.

Palavras-chave: Cifras de Hill; Criptogramas; Decifrar; Sistema Poligráfico.