

Cifras Clássicas e Aplicações em Computação



Cifra de César: funcionamento e exemplo

A *Cifra de César* é uma das técnicas de criptografia mais antigas e utilizadas para introduzir a ideia de codificação. Ela consiste em deslocar cada letra do texto original um número fixo de posições no alfabeto, criando uma mensagem cifrada. Por exemplo, com deslocamento 3, “A” vira “D”, “B” vira “E”, e assim por diante.

Embora hoje seja fácil quebrá-la por sua simplicidade, a Cifra de César é ótima para entender conceitos básicos de segurança e como mensagens podem ser protegidas por meio da transformação dos caracteres. Ela é a porta de entrada para técnicas mais avançadas de criptografia.

Cifra de substituição: conceitos básicos

A *cifra de substituição* funciona trocando cada letra do texto original por outra letra ou símbolo, usando uma tabela pré-definida. Essa troca cria uma mensagem codificada que se torna ilegível para quem não possui a chave correta, reforçando a segurança dos dados.

Ela é uma forma mais elaborada da Cifra de César e uma base importante para criptografia moderna. Mostra como a substituição ajuda a proteger informações de maneira simples e eficaz no mundo digital.

Cifra de transposição: como funciona e usos práticos

Na *cifra de transposição*, as letras da mensagem original não são trocadas, mas sim reorganizadas seguindo uma regra ou padrão específico, como uma troca de linhas por colunas em uma tabela. Isso significa que a mensagem mantém as mesmas letras, mas em posições diferentes.

Esse método é útil para esconder o conteúdo original de forma simples, sendo aplicado em várias situações para aumentar a segurança, especialmente quando combinado com outras técnicas de criptografia.

