Cifra de César

A Cifra de César é uma das mais fáceis e conhecidas técnicas de criptografia. Tratasse de um tipo de cifra de substituição, na qual cada letra de um texto a ser criptografado é substituída por outra letra, presente no alfabeto (26 Letras), porém transportada um certo número de posições à esquerda ou à direita

Benefícios em relação às técnicas anteriores

As técnicas anteriores utilizavam o mesmo método substituição, que é o método usado pelos hebreus, mas substituíam a primeira letra do alfabeto pela última, a segunda pela penúltima e assim sucessivamente invertendo o alfabeto por completo. E que a técnica de César era razoavelmente segura e melhor.

Vulnerabilidade e falhas

A principal vulnerabilidade desse método de criptografia consiste na possibilidade de desincriptação ao se analisar o padrão de frequência dos símbolos. Essa questão já havia sido avaliada antes mesmo da existência do primeiro computador

O que é criptografia?

Criptografia é a prática de codificar e decodificar dados. Quando os dados são criptografados, é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam ser lidos. Os dados só podem ser decodificados ao formato original com o uso de uma chave de decriptografia específica.

Qual seria a função da criptografia?

Trata de um conjunto de regras que mostra codificar a informação de forma que só o emissor e o receptor consigam decifrá-la. Para isso são feitas várias técnicas são usadas, e ao passar do tempo modificada e o surgimento de novas outras de maneira que fiquem mais seguras.

Como uma criptografia protege os usuários?

Em geral, você geralmente tem contato com a criptografia de dados quando precisa inserir informações de identificação pessoal em um formulário da Web. Sites financeiros, do governo, de escolas e de compras costumam criptografar seus dados para ajudar na proteção contra roubo e fraude.