Pesquisa sobre Criptografia

Exemplos Históricos de Uso de Criptografia

Cifra Playfair
A Cifra Playfair é um método de criptografia de substituição que codifica pares de letras em uma matriz 5x5. Desenvolvida no século 19, ela foi amplamente utilizada durante a Primeira Guerra Mundial para enviar mensagens secretas.

Cifras de Substituição
Este tipo de criptografia substitui cada letra do texto original por outra letra ou símbolo. Um exemplo famoso é a Cifra de César, onde cada letra é deslocada um número fixo de posições no alfabeto. Essa técnica foi utilizada por Júlio César para proteger suas comunicações militares.

Algoritmos de Criptografia com Chaves Simétricas

AES (Advanced Encryption Standard)
O AES é um padrão de criptografia amplamente utilizado que oferece alta segurança e eficiência em várias aplicações, sendo a escolha preferida para proteger dados sensíveis em todo o mundo.

Twofish
O Twofish é um algoritmo de cifragem simétrica que se destaca por sua velocidade e segurança. Ele foi finalista na competição para o AES e continua a ser utilizado em diversas aplicações de criptografia.

Algoritmos de Criptografia com Chaves Assimétricas

ECDSA (Elliptic Curve Digital Signature Algorithm)
O ECDSA é um algoritmo de assinatura digital que utiliza curvas elípticas, oferecendo segurança robusta com tamanhos de chave menores. É amplamente utilizado em sistemas de segurança, como transações de criptomoedas.

Diffie-Hellman
O Diffie-Hellman é um método de troca de chaves que permite que duas partes estabeleçam uma chave secreta compartilhada sobre um canal inseguro. Esse protocolo é fundamental para a segurança de comunicação moderna.