Arthur Silva Carvalho

Exemplos

-Cifra de Playfair

Desenvolvida em 1854 por Charles Wheatstone, mas popularizada por Lord Playfair, essa cifra criptográfica utiliza um quadrado 5x5 contendo letras do alfabeto para substituir pares de letras em uma mensagem. Ela foi amplamente utilizada pelos militares britânicos durante a Primeira Guerra Mundial devido à sua simplicidade e eficácia.

-Máquina Enigma

Criada na década de 1920, a Enigma foi uma máquina eletromecânica utilizada pelos nazistas durante a Segunda Guerra Mundial para cifrar mensagens militares. Seu uso proporcionava comunicação segura entre as tropas, até que os Aliados conseguiram decifrar seu código, contribuindo significativamente para o desfecho da guerra.

Algoritmos de Criptografia com Chaves Simétricas Atuais

-AES (Advanced Encryption Standard)

Padrão amplamente utilizado para proteger dados sigilosos.

Adotado pelo governo dos EUA e diversas instituições para segurança da informação.

Utiliza blocos de 128 bits e chaves de 128, 192 ou 256 bits.

-Blowfish

Algoritmo rápido e seguro, utilizado em softwares de segurança e redes.

Suporta chaves variáveis de 32 a 448 bits.

Projetado para ser uma alternativa eficiente a antigos algoritmos de criptografia.

Algoritmos de Criptografia com Chaves Assimétricas Atuais

-RSA (Rivest-Shamir-Adleman)

Muito utilizado para assinaturas digitais e segurança na web.

Baseia-se na dificuldade de fatorização de grandes números primos.

Usado em protocolos como SSL/TLS para segurança na internet.

-ECC (Elliptic Curve Cryptography)

Algoritmo baseado em curvas elípticas, oferecendo segurança com chaves menores.

Utilizado em dispositivos móveis, transações financeiras e aplicações de IoT.

Mais eficiente que RSA em relação ao tamanho da chave e velocidade de operação.