Fernando Porto Estevão

823123863

LAB04

Criptografia: Exemplos Históricos e Algoritmos Atuais

Exemplos Históricos do Uso de Criptografia

1. Código de César (Cifra de César)
   Criada por Júlio César por volta de 58 a.C., essa cifra substituía cada letra do alfabeto por outra deslocada três posições à frente. Por exemplo, “A” virava “D”, “B” virava “E” e assim por diante. Era usada para proteger mensagens militares.
2. Cifra de Vigenère
   Desenvolvida no século XVI, essa cifra polialfabética utilizava uma palavra-chave para criptografar a mensagem com base em várias cifras de César. Por muito tempo, foi considerada “impossível de quebrar” e usada em correspondências sigilosas.

Algoritmos de Criptografia com Chave Simétrica (atualmente usados)

1. AES (Advanced Encryption Standard)
   É o padrão atual de criptografia simétrica, adotado pelo governo dos EUA e amplamente utilizado em sistemas de segurança de dados, como VPNs, criptografia de disco e redes sem fio.
2. ChaCha20
   Um algoritmo de fluxo moderno, muito rápido e seguro, utilizado em aplicativos como o WhatsApp e em conexões seguras (TLS), especialmente em dispositivos móveis, por sua eficiência energética.

Algoritmos de Criptografia com Chave Assimétrica (atualmente usados)

1. RSA (Rivest-Shamir-Adleman)
   Um dos algoritmos mais conhecidos e amplamente usados para criptografia de dados e assinaturas digitais. Baseia-se na dificuldade de fatorar números primos grandes.
2. ECC (Elliptic Curve Cryptography)
   Utiliza curvas elípticas para criar chaves menores e mais seguras, ideal para dispositivos com recursos limitados. É usado em criptografia moderna, como no protocolo HTTPS.