Evolução da Criptografia: Do Passado ao Presente

1. Criptografia na História

Cítala Espartana (c. 700 a.C.)

Um dos primeiros métodos de codificação por transposição. Os espartanos utilizavam uma tira de couro enrolada em um bastão de madeira chamado cítala. A mensagem só podia ser lida corretamente com um bastão do mesmo diâmetro, embaralhando o texto para quem não tivesse a chave física.

Máquina Enigma (1930–1940)

Dispositivo usado pela Alemanha Nazista durante a Segunda Guerra Mundial. Cada letra digitada era transformada por rotores que alteravam constantemente o padrão de substituição, criando uma cifra extremamente complexa. A quebra da Enigma pelos Aliados, liderada por Alan Turing, foi decisiva para o fim da guerra.

2. Criptografia Simétrica

Nesse modelo, a mesma chave é usada para codificar e decodificar a informação.

AES (Advanced Encryption Standard)

Padrão global de segurança utilizado por governos e empresas. Protege redes Wi-Fi (WPA2/3), arquivos com senha e conexões VPN. É considerado altamente seguro.

ChaCha20 / ChaCha20-Poly1305

Algoritmo moderno e eficiente, ideal para dispositivos móveis. Utilizado em conexões HTTPS (TLS 1.3) e adotado por empresas como o Google.

3. Criptografia Assimétrica

Utiliza um par de chaves: uma pública para criptografar e uma privada para decodificar.

RSA (Rivest–Shamir–Adleman)

Baseado na dificuldade de fatorar grandes números primos. Muito usado em assinaturas digitais e na troca segura de informações.

ECC (Elliptic Curve Cryptography)

Mais recente e eficiente, oferece o mesmo nível de segurança do RSA com chaves menores. Ideal para dispositivos com recursos limitados, como smartphones e sensores IoT. Também é utilizado em criptomoedas como o Bitcoin.