Exemplos Históricos do Uso de Criptografia:

César (Croptografia) - 58 a.C.
Descrição: A Cifra de César é uma das formas de criptografia mais antigas conhecidas, creditada a Júlio César, que a empregava para resguardar mensagens militares. A técnica consiste em mover cada letra do alfabeto em um número específico de posições.
Exemplo: Caso a chave seja 3, a letra A se transformaria em D, a letra B em E, e assim sucessivamente.
Significado histórico: A Cifra de César é um método simples de criptografia, sendo vista como um precursor dos sistemas de criptografia atuais.

Máquina Enigma - Segunda Guerra Mundial (1939-1945)

Descrição: Durante a Segunda Guerra Mundial, os nazistas utilizaram a máquina Enigma, uma máquina de codificação, para transmitir mensagens militares cifradas. Ela empregava um sistema de rotinas elétricas para converter texto claro em código, utilizando um conjunto intrincado de combinações de rotores que alteravam a chave de criptografia a cada utilização.
Quebra do Enigma: A decifração do código Enigma pelos aliados, particularmente através do esforço de Alan Turing e sua equipe em Bletchley Park, representou um ponto crucial na história da criptografia. A habilidade de decodificar as mensagens dos nazistas teve um efeito notável na vitória dos aliados.

Importância histórica: A máquina Enigma foi uma das criptografias mais sofisticadas de sua época, e sua quebra é considerada um dos momentos decisivos da guerra, além de ser um dos marcos iniciais para o desenvolvimento da criptografia moderna.

Algoritmos de Criptografia com Chaves Simétricas Utilizados Atualmente:

AES (Standard de Encriptação Avançada)

Descrição: O AES é uma das técnicas de criptografia simétrica mais conhecidas e frequentemente empregadas globalmente. O National Institute of Standards and Technology (NIST) estabeleceu este padrão em 2001 para proteger dados confidenciais do governo americano.

Como opera: O AES emprega uma única chave para criptografar e descriptografar as informações. A chave pode ter dimensões de 128 bits, 192 bits ou 256 bits, com o algoritmo efetuando diversas etapas de transformações matemáticas nos dados para assegurar a proteção.

Aplicações: O AES é empregado em diversas aplicações, tais como a proteção de dados em discos rígidos, comunicações por meio de VPNs, a codificação de documentos e operações financeiras.

DES (Standard de Encriptação de Dados)

Descrição: Em 1977, o governo dos Estados Unidos adotou o padrão de criptografia simétrica conhecido como DES. Ele emprega uma chave de 56 bits e baseia-se em alterações e trocas nos dados em blocos de 64 bits.

Como funciona: O DES executa várias etapas de substituição e troca de dados, utilizando uma chave para criar uma cifra confiável.

Aplicações: Apesar de hoje em dia ser visto como inseguro devido ao seu tamanho reduzido da chave, o DES era frequentemente empregado em protocolos de segurança, como em sistemas bancários e de pagamento, até ser substituído por algoritmos mais robustos, como o AES.

Algoritmos de Criptografia com Chaves Assimétricas Utilizados Atualmente:

Rivest-Shamir-Adlet (RSA)

Descrição: O RSA é um dos algoritmos de criptografia de chave pública (assimétrica) mais antigos e famosos, criado em 1977. Ele emprega duas chaves: uma pública para criptografar as informações e uma privada para descriptografá-las.

Como opera: A confiabilidade do RSA se fundamenta na complexidade de fatorar grandes números compostos. A chave pública pode ser disseminada sem restrições, contudo, a chave privada precisa ser mantida confidencial.

Usos: RSA é frequentemente empregado para garantir a segurança na troca de chaves em protocolos como o SSL/TLS, assegurando a proteção em operações online, como no HTTPS.

ECC (Criptografia de Curva Elíptica)

Descrição: A Criptografia de Curvas Elípticas (ECC) consiste em uma série de algoritmos de chave pública que se baseiam em questões matemáticas que envolvem curvas elípticas. Ela proporciona a mesma proteção que o RSA, porém com chaves consideravelmente menores, o que a torna mais eficaz.

Como opera: O ECC emprega operações algébricas em curvas elípticas para produzir pares de chaves públicas e privadas. Assim, é possível assegurar a segurança das transações com um volume reduzido de dados e processamento.

Aplicações: O ECC é empregado em protocolos como o ECDSA (Algoritmo de Curva Elíptica de Assinatura Digital) e o ECDH (Algoritmo de Curva Elíptica de Diffie-Hellman) para a troca segura de chaves em comunicação criptografada, sendo particularmente eficaz em aparelhos móveis e em cenários com limitações de processamento.