Kauã da Silva Barbosa

Exemplos históricos do uso de criptografia

1-Escítala Espartana

Os espartanos usavam um bastão chamado scytale. Uma tira de couro ou pergaminho era enrolada no bastão, e a mensagem era escrita ao longo dele. Quando desenrolada, as letras pareciam embaralhadas. E somente quem tivesse um bastão do mesmo diâmetro era capaz de ler a mensagem criptografada.

2-One-time pad

Durante a Guerra Fira, agentes de espionagem usavam o método do One-time Pad (OTP). Ele consistia em uma chave secreta totalmente aleatória, usada apenas uma vez para cifrar e decifrar mensagens. Quando aplicado corretamente, esse método é considerado inquebrável matematicamente. A KGB, a CIA e outas agências faziam uso extensivo desse sistema em comunicações secretas.

Citar 2 algoritmos de criptografia com chaves simétricas utilizados atualmente

1-DES (Data Encryption Standard)
O DES foi desenvolvido nos anos 1970 e se tornou um marco na criptografia simétrica, usando blocos de 64 bits e uma chave de 56 bits. Com o avanço da computação, tornou-se vulnerável a ataques de força bruta. Para aumentar a segurança, surgiu o 3DES, que aplica o DES três vezes com chaves diferentes. Embora mais seguro que o DES original, é mais lento e atualmente é usado apenas em sistemas legados, como caixas eletrônicos antigos e algumas transações bancárias.

2-AES (Advanced encryption Standard)

O AES é um algoritmo de criptografia simétrica criado no final dos anos 1990 para substituir o DES. Ele utiliza blocos de 128 bits e chaves de 128, 192 ou 256 bits, combinando permutações e misturas em várias rodadas para garantir a segurança. Sua velocidade e robustez o tornaram o padrão mundial, sendo usando em comunicações seguras, como HTTPS, VPNS, redes Wi-Fi modernas e criptografia de arquivos.

Citar 2 algoritmos de criptografia com chaves assimétricas utilizados atualmente

1-RSA (Rivest-Shamir-Adleman)

O RSA, criado em 1977, é um algoritmo de criptografia assimétrica que permite a comunicação segura sem que remetente e destinatário compartilhem previamente uma chave secreta. Ele utiliza uma chave pública para criptografar e uma chave privada para descriptografar mensagens, sendo baseado na dificuldade de fatorar números grandes. É amplamente usado em certificados digitais, assinaturas eletrônicas, e-mails seguros e protocolos HTTPS.

2- **ECC (Elliptic Curve Cryptography)**

O ECC surgiu nos anos 1980 e ganhou popularidade no século XXI por oferecer alta segurança usando chaves menores, ideal para dispositivos com recursos limitados. Baseia-se em operações matemáticas sobre curvas elípticas, cuja segurança depende da dificuldade do problema do logaritmo discreto na curva. É usado em criptomoedas, autenticação móvel, certificados digitais modernos e protocolos de comunicação segura, oferecendo eficiência e proteção equivalente ao RSA, mas com menos processamento.