Atividades Professor Calvetti- Davi Emanuel Silva Adriano 823149648

ATIVIDADE LAB4

Uso Histórico da Criptografia e Algoritmos Atuais

Exemplos Históricos do Uso da Criptografia

Escítala Espartana (Século V a.C.)

A escítala era um método de criptografia usado pelos espartanos para transmitir mensagens secretas durante a guerra. O sistema consistia em uma fita de couro ou papiro enrolada em um bastão cilíndrico. Ao escrever a mensagem sobre a fita enrolada, as letras ficavam desalinhadas quando a fita era desenrolada, tornando a mensagem ilegível sem um bastão de mesmo diâmetro. Esse método proporcionava uma forma primitiva, mas eficaz, de cifra de transposição.

Código de Beale (Século XIX)

O Código de Beale é um conjunto de mensagens criptografadas que supostamente contém instruções para encontrar um tesouro enterrado nos Estados Unidos. Os documentos foram escritos usando um método de cifra baseada em um texto-chave, onde números representam palavras específicas em um texto de referência. Até hoje, apenas uma das mensagens foi decifrada, tornando esse um dos maiores mistérios da criptografia.

Algoritmos de Criptografia com Chaves Simétricas

AES (Advanced Encryption Standard)

O AES é um dos algoritmos mais usados atualmente para proteção de dados. Ele opera com blocos de 128 bits e suporta chaves de 128, 192 e 256 bits. Amplamente

utilizado em comunicações seguras, armazenamento de dados e proteção de informações sigilosas.

Blowfish

Blowfish é um algoritmo de cifra de bloco criado como uma alternativa ao DES. Ele utiliza chaves variáveis de 32 a 448 bits e é conhecido por sua velocidade e segurança. É usado principalmente em aplicações de segurança e criptografia de senhas.

Algoritmos de Criptografia com Chaves Assimétricas

RSA (Rivest-Shamir-Adleman)

O RSA é um dos algoritmos mais conhecidos de criptografia assimétrica. Baseia-se na fatoração de números primos muito grandes, tornando a quebra do sistema inviável com a tecnologia atual. É amplamente utilizado em assinaturas digitais, certificados SSL/TLS e segurança na internet.

ECC (Criptografia de Curvas Elípticas)

ECC é um método de criptografia assimétrica que oferece segurança semelhante ao RSA, mas com chaves menores, o que o torna mais eficiente. É amplamente usado em dispositivos móveis, pagamentos eletrônicos e redes seguras.