Atividade Prática 04

Angelo Rodrigues 824139676

Cauã de Cerqueira Ferreira 824110637

Erick Domingues Soares 82414486

Wellington de Oliveira Sousa 8241445818

Exemplos Históricos de Uso de Criptografia

1. **Criptografia durante a Guerra Civil Americana: Cifra de Jefferson**
    - Thomas Jefferson, um dos pais fundadores dos Estados Unidos, desenvolveu um dispositivo de criptografia em 1795 que utilizava uma roda de letras rotativas. Essa cifra foi utilizada para proteger comunicações durante a Guerra Civil Americana, permitindo que mensagens militares fossem enviadas de forma segura entre oficiais.
2. **Criptografia na Primeira Guerra Mundial: Cifras de Substituição**
    - Durante a Primeira Guerra Mundial, vários países usaram cifras de substituição para proteger suas comunicações. Um exemplo notável foi o uso da cifra de substituição simples pelo Exército Britânico, que substituía letras por outras letras ou símbolos. Isso foi crucial para manter a comunicação entre os comandantes e suas tropas.

Algoritmos de Criptografia com Chaves Simétricas

1. **Blowfish**
    - Blowfish é um algoritmo de criptografia simétrica que foi projetado para ser rápido e seguro. Ele utiliza uma chave variável que pode ter de 32 a 448 bits e é frequentemente utilizado em softwares de segurança e criptografia de dados.
2. **Twofish**
    - Twofish é o sucessor do Blowfish e também é um algoritmo de criptografia simétrica. Ele opera em blocos de 128 bits e suporta chaves de até 256 bits. Twofish é conhecido por sua velocidade e segurança, sendo uma opção popular para aplicações que exigem criptografia robusta.

Algoritmos de Criptografia com Chaves Assimétricas

1. **DSA (Digital Signature Algorithm)**
    - O DSA é um padrão de assinatura digital utilizado para garantir a autenticidade de uma mensagem. Ele é amplamente utilizado em aplicações que requerem segurança em transações eletrônicas e autenticação.
2. **ElGamal**
    - O algoritmo ElGamal é utilizado para criptografia de chave pública e é baseado na dificuldade do problema do logaritmo discreto. É frequentemente utilizado em sistemas de assinatura digital e em protocolos de troca de chaves.