**Aula 04 – Atividade criptografia**

Nome: Bruno Rodrigues Reis

RA: 8222243147

**Uso Histórico da Criptografia**

A criptografia tem sido utilizada ao longo da história para garantir a segurança da informação. A seguir, são apresentados dois exemplos históricos relevantes:

1. **Escítala Espartana**
   * Data: Cerca de 500 a.C.
   * Descrição: Os espartanos utilizavam um dispositivo chamado "escítala", que consistia em um bastão cilíndrico no qual uma tira de couro ou papiro era enrolada. A mensagem era escrita longitudinalmente na tira, e ao desenrolá-la, o texto tornava-se ilegível. Somente quem tivesse um bastão de mesmo diâmetro poderia ler a mensagem corretamente ao enrolá-la novamente.
2. **Cifra de Jefferson**
   * Data: Final do século XVIII
   * Descrição: Thomas Jefferson criou um dispositivo chamado "Cilindro de Jefferson", composto por vários discos giratórios com letras gravadas em suas bordas. Ao girar os discos de maneira adequada, uma mensagem codificada podia ser lida em uma linha do cilindro. Esse método foi posteriormente adotado pelo exército dos EUA no início do século XX.

**Algoritmos de Criptografia com Chaves Simétricas**

1. **AES (Advanced Encryption Standard)**
   * Descrição: O AES é um dos algoritmos de criptografia mais utilizados atualmente. Ele usa chaves de 128, 192 ou 256 bits e é amplamente empregado para proteger informações sigilosas em comunicações seguras, armazenamento de dados e sistemas de autenticação.
2. **SEAL (Software-Optimized Encryption Algorithm)**
   * Descrição: O SEAL é um algoritmo de cifra de fluxo desenvolvido para alta eficiência em software. Ele utiliza uma estrutura de geração de chave derivada de uma PRNG (Pseudo-Random Number Generator), tornando-o extremamente rápido e adequado para aplicações que exigem alto desempenho.

**Algoritmos de Criptografia com Chaves Assimétricas**

1. **RSA (Rivest-Shamir-Adleman)**
   * Descrição: O RSA é um dos algoritmos de criptografia assimétrica mais utilizados no mundo. Ele se baseia na fatorização de números primos grandes e é amplamente empregado para assinaturas digitais e transmissão segura de dados.
2. ECC (Elliptic Curve Cryptography)
   * Descrição: A criptografia de curva elíptica (ECC) é um método mais eficiente em termos de desempenho e segurança em comparação com o RSA. Ela é amplamente utilizada para segurança em dispositivos móveis, comunicações seguras na internet e blockchain.

Esses algoritmos e exemplos históricos demonstram a evolução da criptografia ao longo dos séculos e sua importância para a segurança da informação nos dias atuais.