Atividade Proposta – Criptografia

1. Dois exemplos históricos do uso de criptografia

1. **Cifra de César (Império Romano)**
- Utilizada por Júlio César para enviar mensagens militares secretas.
- Consistia em deslocar as letras do alfabeto um número fixo de posições (por exemplo, A → D).
- É um dos métodos de criptografia mais antigos e simples.

2. **Máquina Enigma (Segunda Guerra Mundial)**
- Usada pela Alemanha nazista para criptografar mensagens militares.
- Funcionava com rotores que trocavam letras por outras de forma complexa, criando milhões de combinações possíveis.
- Foi quebrada por Alan Turing e sua equipe, o que ajudou os Aliados a vencer a guerra.

2. Dois algoritmos de Criptografia com Chaves Simétricas (atuais)

1. **AES (Advanced Encryption Standard)**
- Amplamente usado em bancos, comunicações seguras e aplicativos de mensagens.
- É rápido e considerado muito seguro.

2. **DES (Data Encryption Standard) / 3DES (Triple DES)**
- DES foi um dos primeiros padrões, mas tornou-se inseguro com o tempo.
- O 3DES surgiu como melhoria, aplicando o DES três vezes para aumentar a segurança.

3. Dois algoritmos de Criptografia com Chaves Assimétricas (atuais)

1. **RSA (Rivest-Shamir-Adleman)**
- Baseado na dificuldade de fatorar números grandes.
- Usado em conexões seguras na internet (HTTPS), certificados digitais e assinaturas eletrônicas.

2. **ECC (Elliptic Curve Cryptography)**
- Usa propriedades matemáticas de curvas elípticas.
- Oferece a mesma segurança que o RSA, mas com chaves menores, sendo mais eficiente em dispositivos móveis e IoT.