Atividade Aula 04

- **Kauê Soares Dos Santos - 824117267**
- **Leonardo Macedo Camargo - 82422817**
- **Luiz Washington de Jesus Muraro - 824148694**
- **Lucas Felipe Monteiro Suarez - 824138683**
- **George Geronimo Menezes Ferreira - 824148488**

Escolher 2 (dois) exemplos históricos do uso de criptografia não citados neste material;

Usos históricos de criptografia:

Código Navajo (Durante a Segunda Guerra Mundial).

Os Estados Unidos utilizaram a língua navajo como base para um código de comunicação secreto. Os "codetalkers" Navajo traduziam mensagens militares em sua língua nativa, que era extremamente difícil de decifrar para os inimigos, já que poucos fora da comunidade Navajo falavam ou entendiam o idioma. Esse código foi usado com grande sucesso pelas forças americanas, especialmente no teatro do Pacífico, e permaneceu indescifrável durante toda a guerra.

Cifra Playfair (Criada em 1854 por Charles Wheatstone).

A Cifra Playfair foi o primeiro método prático de criptografia de dígrafos (pares de letras) em vez de letras individuais. Isso tornava a análise de frequência mais difícil, já que cada par de letras na mensagem era criptografado como uma unidade. A cifra Playfair foi usada pelas forças britânicas na Guerra dos Bôeres e na Primeira Guerra Mundial para transmitir mensagens seguras. Embora mais segura do que as cifras de substituição simples, a cifra Playfair ainda era vulnerável a certos tipos de ataques, mas representou um avanço significativo em técnicas de criptografia manual.

Códigos de Substituição Maias.

Os antigos maias usavam sistemas de escrita complexos que incluíam elementos criptográficos em suas inscrições. Um exemplo é o uso de glifos de substituiçã**o** em seus textos, onde certos símbolos eram usados para representar sons ou palavras de forma indireta, criando um código que só aqueles com conhecimento específico poderiam entender. Embora não fosse criptografia no sentido moderno, essa forma de escrita escondia o verdadeiro significado de textos religiosos e políticos, exigindo um conhecimento especializado para decifrar. É um exemplo primitivo de ocultação de informações em culturas antigas.

Citar 2 algoritmos de Criptografia com Chaves Simétricas utilizados atualmente;

Algoritmos de Criptografia com Chaves Simétricas utilizados atualmente:

- **AES (Advanced Encryption Standard - Padrão de Criptografia Avançada)**.
  É o algoritmo simétrico mais usado hoje em dia, adotado pelo governo dos EUA e amplamente utilizado em segurança de dados. Ele oferece diferentes tamanhos de chave (128, 192 e 256 bits) e é conhecido por sua eficiência e segurança.

- **3DES (Triple DES - Data Encryption Standard - Padrão de Criptografia de Dados)**
  É uma variação do DES que aplica o algoritmo três vezes com três chaves diferentes, proporcionando maior segurança em comparação com o DES simples. Geralmente utilizado em sistemas de pagamento (cartões de crédito) e em alguns sistemas bancários legados.

- **RC4 (Rivest Cipher 4)**:

  Um algoritmo de fluxo bastante utilizado em protocolos como o SSL/TLS, WPA e WEP (criptografia de Wi-Fi). Embora seja eficiente, descobertas de vulnerabilidades reduziram seu uso em novas implementações.

Citar 2 algoritmos de Criptografia com Chaves Assimétricas utilizados atualmente;

Algoritmos de Criptografia com Chaves Assimétricas utilizados atualmente:

DSA (Digital Signature Algorithm - Algoritmo de Assinatura Digital):

- Usado principalmente para criar assinaturas digitais em documentos eletrônicos.

RSA (Rivest-Shamir-Adleman):

- **Descrição**: Um dos algoritmos de criptografia assimétrica mais antigos e amplamente utilizados. Baseia-se na dificuldade de fatoração de números grandes.
- **Uso**: Criptografia de dados, assinaturas digitais, e troca de chaves.

ECC (Criptografia de Curva Elíptica):

- **Descrição:** Oferece alta segurança com chaves menores, sendo amplamente utilizado em dispositivos móveis e IoT, além de também ser utilizado em assinaturas digitais e criptografia de dados.
- **Uso:** seu uso eficiente de recursos, é ideal para dispositivos com capacidade limitada, garantindo segurança em redes conectadas.