* Escolher 2 (dois) exemplos históricos do uso de criptografia não citados neste material;
* Citar 2 algoritmos de Criptografia com Chaves Simétricas utilizados atualmente;
* Citar 2 algoritmos de Criptografia com Chaves Assimétricas utilizados atualmente;

**Exemplos Históricos do Uso de Criptografia**

1. **Criptografia de César:**

* Descrição: A cifra de César é uma das técnicas de criptografia mais antigas e simples empregadas por Júlio César para proteger mensagens militares. Nesse método, cada letra do alfabeto é deslocada para um número fixo de posições (geralmente três) para a direita. Por exemplo, a letra "A" seria "D"

1. **Cifra de Playfair:**

* Descrição: A cifra Playfair, criada por Charles Wheatstone em 1854, utiliza um par de letras para codificar as mensagens. Ao invés de codificar letras individuais, a cifra de Playfair trabalha com digramas (pares de letras) Uma tabela 5x5 é criada a partir de uma palavra-chave, onde as letras estão dispostas. As mensagens são criptografadas, trocando cada par de letras de acordo com as regras da tabela.

**Algoritmos de Criptografia com Chaves Simétricas Utilizados Atualmente**

1. AES (Advanced Encryption Standard):

* Descrição: O algoritmo de criptografia simétrica AES é amplamente empregado na proteção de informações. Para criptografar informações em blocos de 128 bits, ele emprega chaves de 128, 192 ou 256 bits. É considerado seguro e eficiente, sendo empregado em diversas aplicações, incluindo VPNs e criptografia de dados em dispositivos móveis.

1. ChaCha20:

* Descrição: ChaCha20 é um programa de cifra de fluxo criado por Daniel J. Bernstein em 2008. É uma variação do Salsa20 e foi projetado para ser rápido e seguro. Utiliza uma chave de 256 bits e um nonce de 64 bits, permitindo uma ampla gama de operações de criptografia em alta velocidade.

**Algoritmos de Criptografia com Chaves Assimétricas Utilizados Atualmente**

1. RSA (Rivest-Shamir-Adleman):

* Descrição: O RSA é um dos algoritmos de criptografia assimétrica mais empregados. Baseia-se na dificuldade de somar grandes quantidades primordiais. Usa duas chaves: uma para criptografar dados e uma privada para descriptografá-los. É amplamente empregado em comunicações seguras e assinatura eletrônica.

1. ElGamal

* Descrição: O algoritmo ElGamal é um sistema de criptografia assimétrica que se baseia na dificuldade do problema do logaritmo discreto. Ele usa duas chaves: uma para criptografia pública e uma para descriptografia privada. O ElGamal não só permite a troca de chaves, como também pode ser usado para assinaturas digitais.