1. Dois exemplos históricos do uso de criptografia (não citados antes)

1. **Cifras de Júlio César (cerca de 50 a.C.)**
    - Júlio César usava uma técnica simples para comunicar-se com seus generais: cada letra do alfabeto era substituída por outra, deslocada um número fixo de posições (exemplo: A→D, B→E, etc., com deslocamento de 3).
    - É um dos primeiros registros de uso militar da criptografia.
2. **Cifra de Vigenère (século XVI)**
    - Desenvolvida pelo diplomata francês Blaise de Vigenère.
    - Diferente da cifra de César, usava uma **palavra-chave** para determinar múltiplos deslocamentos, tornando a criptografia mais resistente a ataques de frequência.
    - Foi considerada "inviolável" por séculos.

2. Dois algoritmos de Criptografia de Chaves Simétricas usados atualmente

1. **AES (Advanced Encryption Standard)**
    - Muito utilizado em bancos de dados, comunicações seguras (TLS/SSL, VPNs) e armazenamento de arquivos.
    - É o padrão oficial de criptografia dos EUA desde 2001.
2. **DES/3DES (Data Encryption Standard / Triple DES)**
    - O DES original (1977) foi substituído pelo **3DES**, que aplica o algoritmo três vezes em sequência para aumentar a segurança.
    - Hoje é menos usado, mas ainda aparece em sistemas legados e compatibilidade.
    -

3. Dois algoritmos de Criptografia de Chaves Assimétricas usados atualmente

1. **RSA (Rivest–Shamir–Adleman)**
    - Amplamente usado para troca segura de chaves, assinaturas digitais e certificados SSL/TLS.
    - Baseado na dificuldade de fatorar números grandes.
2. **ECC (Elliptic Curve Cryptography)**

- Utiliza propriedades matemáticas de curvas elípticas para fornecer alta segurança com chaves menores (mais eficiente que RSA).
- Usado em dispositivos móveis, certificados digitais modernos e criptomoedas.