1. **Exemplos Históricos de Criptografia**

- A Cítala Espartana (c. 700 a.C.):

- **Um dos primeiros métodos de criptografia por transposição. Os espartanos usavam um bastão de madeira — a *cítala* — como chave. A mensagem era escrita em uma tira de couro enrolada ao redor do bastão. Ao desenrolar, o texto ficava embaralhado, só podendo ser lido novamente com um bastão do mesmo diâmetro.**

- A Máquina Enigma (1930–1940):

- **Utilizada pela Alemanha Nazista na Segunda Guerra Mundial, a Enigma é um exemplo de criptografia por substituição polialfabética. Cada letra digitada passava por rotores elétricos que mudavam constantemente o alfabeto de substituição, tornando o código extremamente complexo. A quebra da Enigma pelos Aliados — liderada por Alan Turing — foi decisiva para o desfecho da guerra.**

2. **Algoritmos de Criptografia Simétrica**

- **AES (Advanced Encryption Standard)**
  Padrão mundial de criptografia, usado por governos e empresas. Presente em redes Wi-Fi (WPA2/3), arquivos protegidos por senha e VPNs, o AES é considerado extremamente seguro.

- **ChaCha20 (ou ChaCha20-Poly1305)**
  Algoritmo moderno otimizado para dispositivos móveis. É amplamente usado em conexões seguras via HTTPS (TLS 1.3) e adotado por grandes empresas como o Google.

3. **Algoritmos de Criptografia Assimétrica**

- **RSA (Rivest–Shamir–Adleman)**
  Baseado na dificuldade de fatorar números primos muito grandes, o RSA é um dos algoritmos mais tradicionais. É amplamente usado em assinaturas digitais e trocas seguras de chaves.

- **ECC (Elliptic Curve Cryptography)**
  Mais recente e eficiente, o ECC oferece o mesmo nível de segurança do RSA com chaves menores, sendo ideal para dispositivos móveis e IoT. Também é utilizado em criptomoedas como o Bitcoin.