

## Pesquisa sobre Criptografia – Exemplos Históricos e Algoritmos Modernos

A criptografia é uma técnica fundamental para proteger informações ao longo da história. Neste trabalho, serão apresentados dois exemplos históricos relevantes, bem como algoritmos modernos de criptografia simétrica e assimétrica.

### Exemplos Históricos

- **Cifra de César:** Método usado pelo imperador romano Júlio César, baseado na substituição de letras por outras deslocadas no alfabeto. Foi um dos primeiros exemplos de criptografia documentados.
- **Máquina Enigma:** Dispositivo utilizado pela Alemanha nazista durante a Segunda Guerra Mundial. A máquina embaralhava mensagens de forma complexa, e sua quebra pelos Aliados, com ajuda de Alan Turing, foi decisiva para a vitória.

### Criptografia com Chaves Simétricas

- **AES (Advanced Encryption Standard):** Algoritmo padrão de segurança utilizado em sistemas bancários, internet e dispositivos móveis. É considerado um dos mais seguros atualmente.
- **3DES (Triple Data Encryption Standard):** Evolução do DES, ainda presente em sistemas legados. Aplica três vezes o algoritmo DES, aumentando a segurança.

### Criptografia com Chaves Assimétricas

- **RSA (Rivest–Shamir–Adleman):** Baseado em operações matemáticas com números primos grandes. Usado em assinaturas digitais e troca de chaves.
- **ECC (Elliptic Curve Cryptography):** Baseado em curvas elípticas. Oferece alta segurança com chaves menores, sendo muito usado em dispositivos móveis e certificados digitais.

### Conclusão

A criptografia evoluiu de técnicas simples, como a Cifra de César, para algoritmos altamente sofisticados como AES, RSA e ECC. Ela é essencial para a segurança digital e continuará evoluindo conforme surgem novas ameaças.