

Fábio Henrique Santos Marano - USTJ

RA : 825111150

1. Exemplos históricos de criptografia

- Cifra de César: Júlio César usava essa técnica para esconder mensagens. Ele basicamente trocava cada letra por outra algumas posições à frente no alfabeto.
- Máquina Enigma: Era usada pelos nazistas na Segunda Guerra para criptografar mensagens. Os Aliados, com a ajuda de Alan Turing, conseguiram decifrá-la e isso ajudou a ganhar a guerra.

2. Algoritmos de criptografia com chaves simétricas

- AES: Um dos mais seguros atualmente, usado para proteger dados na internet, bancos, etc.
- DES: Foi muito usado no passado, mas ficou fraco com o avanço da tecnologia e foi substituído pelo AES.

3. Algoritmos de criptografia com chaves assimétricas

- RS: Muito usado na internet, especialmente em sites seguros (HTTPS), porque usa um par de chaves (uma pública e outra privada).
- ECC: Faz a mesma coisa que o RSA, mas é mais eficiente e ocupa menos espaço, sendo ótimo para celulares e dispositivos com menos poder de processamento.