criptografia

· **Máquina Enigma (segunda guerra mundial)**

A Máquina Enigma era usada pelos nazistas na Segunda Guerra para criptografar mensagens. Ela funcionava como uma máquina de escrever, mas com um sistema de rotores que trocavam as letras da mensagem original por outras, de forma diferente a cada dia. Isso tornava a criptografia super difícil de quebrar.

Os britânicos, liderados por Alan Turing, criaram uma máquina chamada Bombe, que testava várias combinações para descobrir a configuração diária da Enigma. Ao decifrar essas mensagens, os Aliados conseguiram antecipar ataques e mudar o rumo da guerra.

· **Código Navajo (segunda guerra mundial)**

Durante a Segunda Guerra, os Estados Unidos usaram a língua **Navajo** como um código secreto para enviar mensagens militares. Como o Navajo era um idioma pouco conhecido e sem forma escrita, já era difícil de entender por si só. Além disso, os "Code Talkers" criaram um sistema onde palavras comuns representavam termos militares (por ex: "tartaruga" significava tanque)

Os japoneses nunca conseguiram decifrar esse código, pois mesmo que capturassem uma mensagem, sem um falante Navajo era impossível de entender. Esse método foi essencial para as vitórias americanas no Pacífico, tornando as comunicações seguras e rápidas.

• **Criptografia com Chaves Simétricas**

1. **AES (Advanced Encryption Standard)** – Muito seguro e usado em redes wi-fi e proteção de dados, com chave de até 256 bits

2. **ChaCha20** - Algoritmo de fluxo rápido e seguro, usado no protocolo TLS (para conexões seguras na internet) e em aplicativos como o Signal. Ele é uma alternativa ao AES, especialmente em dispositivos móveis, por ser eficiente e resistente a ataques.

• **Criptografia com Chaves Assimétricas**

1. **RSA** – Amplamente utilizado em transmissões seguras na internet, como em certificados SSL/TLS. Baseia-se na fatoração de números primos grandes.

2. **ECC (Elliptic Curve Cryptography)** – Mais eficiente que o RSA, usado em criptografia moderna, incluindo blockchain e dispositivos móveis.