Fundamentos de Criptografia de dados

CAIO BARBOSA - 825154397
EDUARDA MOLINA - 825154538
JULIA RICHELLY - 825150438
KARLA SANTOS - 825149900

Criptografia

- Scytale Espartana (cerca de 400 a.C.)

Utilizada pelos espartanos em campanhas militares. Era um bastão cilíndrico em torno do qual se enrolava uma tira de couro ou pergaminho. A mensagem só podia ser lida quando enrolada em um bastão de mesmo diâmetro.

- Código Navajo (Segunda Guerra Mundial)

Os Estados Unidos utilizaram a língua Navajo como código, pois era extremamente difícil de decifrar para os inimigos. Os “Code Talkers” (faladores de código) foram fundamentais para as comunicações militares no Pacífico.

Criptografia com Chaves Simétricas

- AES (Advanced Encryption Standard) – usado em comunicações seguras, VPNs, discos criptografados etc.
- DES/3DES (Data Encryption Standard / Triple DES) – embora o DES esteja obsoleto, o 3DES ainda aparece em sistemas legados.

Criptografia com Chaves Assimétricas

- RSA (Rivest–Shamir–Adleman) – muito utilizado em certificados digitais, SSL/TLS, assinaturas digitais.
- ECC (Elliptic Curve Cryptography) – baseado em curvas elípticas, fornece alta segurança com chaves menores, sendo usado em dispositivos móveis, blockchain e sistemas modernos.