UNIVERSIDADE SÃO JUDAS TADEU

Emilly dos santos ferreira
RA: 825153657

Sistemas computacionais e segurança

Professor Robson Calvetti

Sao Paulo - 2025

• Exemplos históricos da Criptografia

RSA e a Revolução Digital (1977)

O algoritmo RSA, criado por Rivest, Shamir e Adleman, trouxe a criptografia moderna de chave pública, permitindo comunicações seguras na internet, como usamos hoje em bancos e e-mails.

A criptografia evoluiu de métodos simples para algoritmos altamente sofisticados, sendo essencial para a segurança digital no mundo atual!

Código Navajo (Segunda Guerra Mundial)

Os EUA usaram a língua Navajo como base para um código secreto. Como o idioma era pouco conhecido fora das tribos indígenas e não tinha forma escrita, os japoneses nunca conseguiram decifrá-lo.

• Algoritmos de criptografia com chaves simétricas utilizados atualmente

AES (Advanced Encryption Standard)

- O mais popular e seguro atualmente
- Utiliza chaves de 128, 192 ou 256 bits
- Muito usado em bancos, VPNs, Wi-Fi (WPA2/WPA3) e comunicação segura

Blowfish

- Algoritmo rápido e seguro, com chaves de 32 a 448 bits
- Usado em ferramentas como crypt() para armazenamento de senhas
- Foi substituído pelo AES em muitos casos

• Algoritmos de criptografia com chaves assimétricas utilizados atualmente

EdDSA (Edwards-curve Digital Signature Algorithm)

- Variante mais moderna do DSA
- Baseado em curvas elípticas, como o Curve25519
- Mais rápido e seguro contra ataques avançados
- Utilizado em criptografia de e-mails (PGP), SSH e autenticação segura

RSA (Rivest-Shamir-Adleman)

- Mais popular e amplamente utilizado
- Baseado na fatoração de números primos
- Suporta chaves de 1024, 2048 e 4096 bits
- Usado em SSL/TLS, assinaturas digitais e autenticação