

Criptografia

Conceito, objetivo, aplicações e exemplos

Conceito

- Técnica para codificar informações, tornando-as inacessíveis a usuários não autorizados.
- Garante confidencialidade, integridade, autenticidade e não repúdio.

Objetivo

- Proteger dados sensíveis durante o armazenamento ou transmissão.
- Garantir a identidade dos envolvidos na comunicação.

Aplicações

- Transações bancárias online
- Armazenamento de senhas
- Mensageiros instantâneos (WhatsApp, Signal)
- Certificados digitais (HTTPS)
- Blockchain e criptomoedas

Exemplos

- Autenticação com tokens (2FA)
- Comunicação segura em e-mails (PGP)

Tipos de Criptografia

Simétrica

- Alta performance, ideal para grandes volumes de dados
- Vulnerável se a chave for descoberta
- Exemplo
 - AES (Advanced Encryption Standard)

Assimétrica

- Usa duas chaves: pública (distribuída) e privada (secreta)
- Mais segura para comunicação entre partes
- Exemplo
 - ECC (Elliptic Curve Cryptography)
 - RSA (Rivest–Shamir–Adleman)