Criptografia: História, Tipos e Algoritmos Atuais

O que é Criptografia

A criptografia é a ciência de **esconder informações**. Ela transforma mensagens legíveis, chamadas de "texto claro", em mensagens incompreensíveis, chamadas de "texto cifrado". Somente destinatários autorizados, que possuem a chave correta, conseguem ler a mensagem original. A criptografia moderna combina técnicas matemáticas avançadas com o uso de chaves secretas, mas técnicas simples de substituição ou transposição também foram usadas historicamente.

Exemplos Históricos de Criptografia

Cifra Atbash (século V a.C.)

A Cifra Atbash é uma técnica antiga usada pelos hebreus. Ela funciona substituindo cada letra do alfabeto pela sua **oposta**, por exemplo, a primeira letra se torna a última, a segunda se torna a penúltima, e assim por diante. Essa técnica permitia que mensagens religiosas ou militares fossem compreendidas apenas por quem conhecia a lógica da cifra.

Códigos Navajo (Segunda Guerra Mundial)

Durante a Segunda Guerra Mundial, os Estados Unidos criaram códigos militares baseados na língua navajo. Mensagens estratégicas eram traduzidas para o navajo e depois cifradas com códigos adicionais. A combinação da língua pouco conhecida com códigos especiais tornou a comunicação quase impossível de ser decifrada pelos inimigos. Esse método comprovou que **idiomas e códigos humanos** podem ser usados como ferramentas de criptografia.

Criptografia com Chave Simétrica

A criptografia simétrica utiliza **uma única chave** tanto para criptografar quanto para descriptografar informações. É rápida e indicada para grandes volumes de dados, como arquivos de servidores ou comunicação de VPNs.

Algoritmos atuais:

1. **AES (Advanced Encryption Standard):**
   - Usa chaves de 128, 192 ou 256 bits.
   - Muito seguro, usado em bancos, VPNs e sistemas corporativos.
2. **ChaCha20:**
   - Mais rápido em software, ideal para dispositivos móveis.
   - Resistente a ataques mesmo em sistemas com hardware limitado.

Criptografia com Chave Assimétrica

A criptografia assimétrica utiliza **duas chaves diferentes**: uma pública para criptografar dados e uma privada para descriptografá-los. É mais lenta que a simétrica, mas essencial para **transações seguras e autenticação digital**, como assinaturas ou certificados.

Algoritmos atuais:

1. **RSA:**
   - Baseado na dificuldade de fatorar números muito grandes.
   - Usado em certificados HTTPS, autenticação de sites e assinaturas digitais.
2. **ECC (Elliptic Curve Cryptography):**
   - Utiliza curvas matemáticas complexas.
   - Fornece segurança equivalente ao RSA com **menos processamento**, sendo ideal para dispositivos móveis e criptomoedas.

Comparação entre Criptografia Simétrica e Assimétrica

Característica	Simétrica	Assimétrica
Chaves	1 (mesma para criptografar e descriptografar)	2 (pública e privada)
Velocidade	Rápida	Mais lenta
Uso típico	Grandes volumes de dados	Assinaturas, autenticação, pequenas transações
Exemplos de algoritmo	AES, ChaCha20	RSA, ECC

Conclusão

A criptografia é essencial para proteger **sigilo, integridade e autenticidade** de informações. Desde técnicas antigas, como a Cifra Atbash e os códigos Navajo, até os algoritmos modernos AES, ChaCha20, RSA e ECC, a criptografia evoluiu para atender à crescente necessidade de segurança digital. Conhecer os tipos de criptografia e seus algoritmos é fundamental para a proteção de dados pessoais e corporativos no mundo atual.

Gustavo Jaccon Franquini
RA: 825150548