Universidade São Judas Tadeu

Ciência da computação

Atividade Sistemas computacionais e segurança

Lucas de Lima Garcia - 825145166

Professor Orientador

Robson Calvetti

Dois Exemplos Históricos de Criptografia

1. **Os "códigos" dos Incas – Quipus**
   Os Incas tinham um sistema chamado **quipu**, feito de cordas com nós, que era usado para armazenar informações. Apesar de ser mais conhecido como uma ferramenta administrativa, algumas evidências sugerem que certos quipus guardavam mensagens codificadas. Como apenas os **quipucamayocs** (os especialistas em quipus) sabiam interpretar essas informações, esse pode ter sido um método primitivo de criptografia.
2. **A Cifra Nihilist – Segredo dos Revolucionários Russos**
   No século XIX, revolucionários russos usaram a **Cifra Nihilist** para enviar mensagens secretas. Esse método era uma variação da cifra de Vigenère, mas envolvia uma matriz numérica baseada em palavras-chave, tornando a decodificação muito mais difícil. Esse sistema foi usado por grupos que lutavam contra o governo czarista.

Dois Algoritmos de Criptografia Simétrica Usados Hoje

1. **AES – A Fortaleza Digital**
   O **AES (Advanced Encryption Standard)** é um dos algoritmos de criptografia mais seguros do mundo. Ele funciona embaralhando os dados em várias rodadas de substituições e permutações, tornando quase impossível decifrá-los sem a chave certa. É usado em coisas como **armazenamento de dados, VPNs e segurança de bancos**.
2. **ChaCha20 – O Cifrador Rápido e Leve**
   O **ChaCha20** é um algoritmo que embaralha dados de uma maneira diferente, usando operações matemáticas simples, mas muito eficazes. Ele é muito rápido e seguro, sendo preferido para **dispositivos móveis, conexões seguras na internet e até no WhatsApp**.

Dois Algoritmos de Criptografia Assimétrica Usados Hoje

1. **RSA – O Clássico da Segurança Digital**
   O **RSA** é um dos métodos mais antigos e confiáveis para criptografia assimétrica. Ele usa um truque matemático: multiplicar dois números primos gigantes é fácil, mas desfazê-lo (fatoração) é absurdamente difícil. Isso garante segurança para **assinaturas digitais, proteção de e-mails e transações bancárias**.
2. **ECDSA – Segurança com Eficiência**
   O **ECDSA (Elliptic Curve Digital Signature Algorithm)** faz basicamente o que o RSA faz, mas de forma muito mais eficiente. Como usa **criptografia baseada em curvas elípticas**, permite um alto nível de segurança usando chaves bem menores. Ele é muito usado em **Bitcoin, certificados digitais e sistemas modernos de autenticação**.