Universidade São Judas Tadeu

Sistemas Computacionais e Segurança

Prof. Robson Calvetti

João Luiz Da Silva e Rafael Tiago Scisci Arciénega

RA: 82420546 e 824216105

Criptografia

É a técnica onde uma informação é codificada com o intuito de ser protegida, e somente é possível acessá-la quem possuir permissão, normalmente essa permissão ocorre através do uso de chaves digitais.

A criptografia já pode ser considerada uma prática bem antiga, com evidências de uso há mais de 3.900 anos, sendo extremamente importante ao longo da história e desempenhando papéis cruciais em diversos momentos, especialmente em cenários militares, diplomáticos e tecnológicos, como:

Cifra Niilista

A Cifra Niilista é um método criptográfico usada muito por revolucionários russos no século 19, principalmente pelos niilistas, que buscavam derrubar o regime czarista. A partir dessa cifra eles podiam se comunicar sem serem capturados pelas autoridades czaristas.

Esse sistema de cifragem combina técnicas de substituição com números e deriva em parte da cifra de Políbio, um método grego antigo.

Cifra de Bacon

Inventada por Francis Bacon, é uma cifra de substituição binária que usa duas formas diferentes de representação para substituir as letras do alfabeto. As letras são substituídas por grupos de cinco letras A e B, representando a codificação binária de cada letra.

Simétricas

CAMELLIA:

Camellia é um algoritmo de criptografia de bloco desenvolvido no Japão por Mitsubishi e NTT. Ele tem uma estrutura semelhante ao AES e oferece um nível de segurança comparável. Usa chaves de 128, 192 ou 256 bits.

Opera em blocos de 128 bits. Considerado eficiente em software e hardware, sendo especialmente popular em aplicações asiáticas. Camellia é usado em vários protocolos de segurança, como o TLS/SSL e em criptografia de disco.

DES

Data Encryption Standard (DES) é uma das primeiras criptografias utilizadas e é considerada uma proteção básica de poucos bits (cerca de 56). O seu algoritmo é o mais difundido mundialmente e realiza 16 ciclos de codificação para proteger uma informação.

O DES pode ser decifrado com a técnica de força bruta (o programa testa as possibilidades de chave automaticamente durante horas). Por essa razão, os desenvolvedores precisam buscar alternativas de proteção mais complexas além do DES.

ASSIMÉTRICAS:

CRYSTALS-KYBER:

Um algoritmo pós-quântico para troca de chaves baseado em redes euclidianas, parte do projeto NIST de padronização de criptografia quântica, projetado para ser seguro contra ataques de computadores quânticos, oferece troca de chaves rápidas e seguras. Prevê-se que seja utilizado em futuras implementações para resistir a ameaças da computação quântica.

RSA (Rivest-Shamir-Adleman):

RSA é um dos algoritmos mais conhecidos e amplamente utilizados para criptografia assimétrica. Ele se baseia na dificuldade de fatorar números inteiros grandes. É frequentemente utilizado para a troca de chaves e assinatura digital. Quando uma mensagem é criptografada com a chave pública do destinatário, apenas a chave privada correspondente pode descriptografá-la.