Universidade São Judas Tadeu

Sistemas Computacionais e Segurança

CRIPTOGRAFIA E ALGORITIMOS

João Vitor Chioatto Serafim – 825133189

Professor: Robson Calvetti

São Paulo – SP

2025

CASOS HISTÓRICOS DE CRIPTOGRAFIA EM AÇÃO

Guerra Civil Americana: Durante o conflito (1861–1865), os generais Confederados precisavam de um jeito de mandar ordens confidenciais sem o risco de interceptação. A solução era a criptografia manual em papel, com tabelas que substituíam letras ou rearranjavam a ordem das palavras. Cada letra se transformava em outra ou em um símbolo. As mensagens eram manuscritas, e só quem possuía a tabela secreta conseguia lê-las. Se o inimigo pusesse as mãos na tabela, a criptografia perdia a eficácia. O exército do Norte analisou padrões nas mensagens e, assim, decifrou ordens, alterando seus planos de batalha.

Segunda Guerra Mundial – JN-25 na Batalha de Midway: Na Segunda Guerra Mundial, os japoneses usavam o código JN-25 para enviar mensagens secretas. Cada palavra ou frase correspondia a um número em um livro de códigos, e um outro número secreto era adicionado para dificultar ainda mais a decifração. As mensagens eram transmitidas por rádio e só podiam ser decifradas por quem tinha os livros e a chave correta. Os americanos estudaram os padrões, conseguiram decifrar a criptografia JN-25 e descobriram que Midway seria o alvo, preparando uma emboscada decisiva.

Algoritmos de Criptografia com Chaves Simétricas (a mesma chave para criptografar e descriptografar)

Twofish: É um método de criptografia que emprega a mesma chave tanto para proteger quanto para acessar informações. Opera com blocos de 128 bits e aceita chaves grandes (até 256 bits). É ágil e confiável, presente em softwares como o VeraCrypt para a proteção de arquivos e discos.
Exemplo: No VeraCrypt, o Twofish pode ser usado para criar um disco virtual criptografado no computador, resguardando documentos pessoais com uma senha.

IDEA: Também utiliza a mesma chave para criptografar e descriptografar, sendo criado na Suíça. Realiza cálculos matemáticos básicos (soma e multiplicação) para ocultar mensagens. Foi amplamente utilizado no PGP, para proteger e-mails, e ainda é considerado seguro em algumas situações.
Exemplo: Ao enviar um e-mail confidencial através do PGP, ele pode ser criptografado com o IDEA, garantindo que somente o destinatário com a chave correta possa lê-lo.

Algoritmos de Criptografia com Chaves Assimétricas (chaves distintas para criptografar e descriptografar)

ElGamal: Neste tipo de criptografia, uma chave pública é utilizada para criptografar a mensagem, enquanto uma chave privada a descriptografa. ElGamal é usado principalmente para assinaturas digitais e troca de chaves de forma segura. É um método seguro, embora as mensagens fiquem um pouco maiores.
Exemplo: Alguns sistemas de autenticação em sites e aplicativos empregam o ElGamal para proteger a troca de chaves entre o servidor e o usuário, assegurando que ninguém consiga interceptar a senha.

DSA (Digital Signature Algorithm): O DSA é um algoritmo para assinaturas digitais. Ele assegura que um documento ou mensagem seja genuíno e não tenha sofrido alterações. É bastante utilizado em certificados digitais e sistemas que necessitam comprovar que a informação foi enviada pela pessoa certa.
Exemplo: Ao acessar um site seguro com HTTPS, o certificado digital do site pode utilizar o DSA para demonstrar que o site é legítimo e que os dados transmitidos estão protegidos.