UNIVERSIDADE SÃO JUDAS TADEU

SISTEMAS COMPUTACIONAIS E SEGURANÇA

ALUNOS:

BOAZ MOREIRA CIRINO - RA: 825146412

DANIEL SOUZA BEZERRA - RA: 825158378

EMILYN CARDOSO – RA: 824214832

MICAEL WILLIAM - RA: 824213069

SÃO PAULO
2025

Uso Histórico da Criptografia e Algoritmos Atuais

Introdução

A criptografia tem sido utilizada ao longo da história para proteger informações sigilosas e garantir a comunicação segura. Neste trabalho, apresentaremos dois exemplos históricos do uso da criptografia, além de citar algoritmos simétricos e assimétricos amplamente utilizados nos dias atuais.

Exemplos Históricos de Uso da Criptografia

Escrita Cifrada de Mary, Rainha da Escócia

Mary Stuart, rainha da Escócia no século XVI, utilizava um sofisticado sistema de criptografia para enviar mensagens secretas enquanto estava presa. Suas mensagens eram escritas em uma cifra substitutiva complexa, onde letras eram trocadas por símbolos e números. No entanto, os espiões da Rainha Elizabeth I conseguiram decifrar suas comunicações, o que levou à sua execução em 1587. Esse episódio mostra como a criptografia já era usada para fins políticos e de espionagem na época.

Cifra Maia

Os maias, uma das civilizações mais avançadas da Mesoamérica, desenvolveram um sistema de escrita altamente complexo, que ainda desafia estudiosos. Embora não fosse criptografia no sentido moderno, sua escrita glífica era usada para registrar eventos, previsões astrológicas e informações políticas de maneira que apenas a elite sacerdotal e governante podia interpretar. Por muito tempo, essa escrita permaneceu indecifrável, funcionando como uma forma de proteção da informação, um conceito que remete ao propósito da criptografia.

Algoritmos de Criptografia Atuais

Algoritmos Simétricos

Na criptografia simétrica, a mesma chave é usada para criptografar e descriptografar a mensagem. Dois exemplos de algoritmos amplamente utilizados são:

- AES (Advanced Encryption Standard): Um dos algoritmos mais seguros atualmente, utilizado em diversas aplicações, como comunicações seguras e proteção de dados em armazenamento.
- DES (Data Encryption Standard): Embora tenha sido amplamente utilizado no passado, o DES foi substituído pelo AES devido a vulnerabilidades relacionadas ao aumento da capacidade computacional.

Algoritmos Assimétricos

Na criptografia assimétrica, utilizam-se duas chaves: uma pública para criptografar e uma privada para descriptografar. Dois exemplos comuns são:

- RSA (Rivest-Shamir-Adleman): Um dos algoritmos mais utilizados para comunicações seguras na internet, incluindo transações bancárias e autenticação digital.
- ECC (Elliptic Curve Cryptography): Utiliza curvas elípticas para fornecer segurança equivalente ao RSA, mas com chaves menores, tornando-o mais eficiente em dispositivos com recursos limitados.

Conclusão

A criptografia evoluiu significativamente desde os tempos antigos até os dias atuais. Enquanto métodos históricos como a escrita cifrada de Mary Stuart e a complexa escrita maia ilustram a importância da proteção da informação no passado, os algoritmos modernos, como AES e RSA, garantem a segurança dos dados no mundo digital.