Exemplos de Criptografia

(Prof. Calvetti)

Cifra de Zimmermann:

A Cifra de Zimmermann refere-se à mensagem criptografada enviada pelo ministro das Relações Exteriores da Alemanha, Arthur Zimmermann, ao embaixador alemão no México em janeiro de 1917, durante a Primeira Guerra Mundial. A mensagem, conhecida como o Telegrama Zimmermann, propunha uma aliança militar entre a Alemanha e o México, caso os Estados Unidos entrassem na guerra contra a Alemanha. Em troca, a Alemanha prometia ajudar o México a recuperar territórios perdidos para os EUA, como o Texas, Arizona e Novo México.

O telegrama foi interceptado e decodificado pelos britânicos, que usavam técnicas avançadas de criptografia na época. O serviço de inteligência britânico, conhecido como Room 40, conseguiu quebrar a cifra alemã e decifrar o conteúdo da mensagem, o que foi um golpe crucial para a Alemanha. Após a decodificação, os britânicos repassaram a informação aos

Estados Unidos.

A divulgação do conteúdo do telegrama ao público causou grande indignação nos EUA, fortalecendo o sentimento contra a Alemanha. Isso contribuiu para a decisão do presidente Woodrow Wilson de entrar na guerra em abril de 1917, ao lado dos Aliados.

A Cifra de Zimmermann foi um dos exemplos mais notáveis de como a criptografia e a quebra de códigos tiveram um impacto direto nos eventos históricos, mudando o rumo da Primeira Guerra Mundial.

Como funcionava:

A Cifra de Zimmermann utilizava um método de criptografia baseado em substituição, conhecido como cifra de substituição polialfabética. Cada letra da mensagem original era substituída por outra letra, com base em uma tabela de substituição criada usando uma chave. Essa cifra complexa envolvia múltiplos alfabetos e rotacionava os padrões de substituição, tornando a decodificação mais difícil. A segurança da cifra dependia da complexidade da chave e do método de substituição, mas foi eventualmente quebrada pelos britânicos com técnicas

avançadas de criptografia.

Cifra de Atbash:

A Cifra de Atbash é uma cifra de substituição simples e antiga que foi usada principalmente na criptografia hebraica. Ela consiste em um método de mapeamento onde cada letra do alfabeto é substituída pela sua contraparte oposta. No alfabeto inglês, por exemplo, a letra 'A' é substituída por 'Z', 'B' por 'Y', e assim por diante. O mapeamento é simétrico, ou seja, a mesma tabela de substituição é usada tanto para criptografar quanto para descriptografar a mensagem.

Essa cifra é chamada de "Atbash" devido à sua origem na tradição hebraica, onde foi utilizada para escrever textos criptografados em algumas tradições cabalísticas e textos antigos. O nome "Atbash" deriva da forma como as letras são mapeadas: a primeira letra é substituída pela última, a segunda pela penúltima, e assim por diante.

Apesar de ser uma técnica de criptografia muito simples e

facilmente decifrável com análise de frequência, a Cifra de Atbash foi um avanço significativo na época em que foi criada. Sua simplicidade a torna um exemplo clássico de criptografia antiga e é frequentemente estudada por aqueles interessados na história da criptografia. Embora não seja segura pelos padrões modernos, a Cifra de Atbash oferece um interessante vislumbre das práticas criptográficas antigas.

Como funcionava:

A Cifra de Atbash é uma cifra de substituição onde cada letra do alfabeto é trocada por sua contraparte oposta: 'A' se torna 'Z', 'B' se torna 'Y', e assim por diante. O mapeamento é simétrico, significando que a mesma tabela é usada para criptografar e descriptografar a mensagem. Por exemplo, "HELLO" seria cifrada como "SVOOL". Esta cifra simples é facilmente quebrada por análise de frequência e não oferece segurança robusta para comunicações modernas.

Exemplos de algoritmos de criptografia com chaves simétricas

ChaCha20:

A criptografia ChaCha20 é uma cifra de fluxo simétrica que usa uma chave de 256 bits e um contador de 64 bits para gerar um fluxo pseudoaleatório de bits, que é combinado com os dados para criptografá-los. O algoritmo realiza operações simples como adição, XOR e rotação, tornando-o rápido e eficiente, especialmente em software.

Ela é usada em protocolos TLS como alternativa ao AES para proteger dados em trânsito, além de ser amplamente empregada em VPNs como o WireGuard devido à sua alta performance. Também é eficaz em dispositivos móveis, pois oferece segurança com baixo consumo de energia. ChaCha20 é conhecida por sua velocidade, simplicidade e robustez em diversos sistemas de comunicação.

Blowfish:

A criptografia Blowfish é um algoritmo de cifra simétrica que criptografa dados em blocos de 64 bits, usando chaves de 32 a 448 bits. Desenvolvido para ser rápido e seguro, o Blowfish realiza múltiplas rodadas de substituições e permutações para

transformar o texto em claro em texto cifrado. Ele é amplamente utilizado para proteger dados em trânsito e em repouso, sendo aplicável em criptografia de arquivos e em alguns protocolos de segurança. Embora seja eficaz e flexível, seu uso tem diminuído com a adoção de algoritmos mais modernos como o AES, que oferecem maior segurança e eficiência. Blowfish continua sendo uma opção relevante para sistemas que requerem criptografia de alta performance.

Exemplos de algoritmos de criptografia com chaves Assimétricas

Diffie-Hellman:

A criptografia Diffie-Hellman é um protocolo de troca de chaves que permite que duas partes estabeleçam uma chave secreta compartilhada através de um canal inseguro. Baseado em problemas matemáticos complexos, como o logaritmo discreto, ele garante que ambas as partes possam calcular a mesma chave sem nunca enviar a chave secreta diretamente. O processo envolve a troca de chaves públicas derivadas de uma chave privada, e cada parte usa a chave pública recebida e sua chave privada para calcular a chave compartilhada. Essa chave

é então usada para criptografar comunicações seguras. Diffie-Hellman é amplamente utilizado em protocolos como TLS para garantir a troca segura de chaves de sessão em comunicações na internet.

Lattice-Based Cryptography:

Lattice-Based Cryptography é uma abordagem criptográfica que se baseia em problemas matemáticos complexos relacionados a redes (lattices), como o problema do vetor mais curto e o problema da base mais curta. Esses problemas são considerados difíceis de resolver, mesmo para computadores quânticos, oferecendo uma segurança robusta contra ataques futuros. O funcionamento envolve gerar chaves públicas e privadas usando transformações matemáticas dessas redes e aplicar essas chaves em esquemas de criptografia e assinaturas digitais. É especialmente relevante para a segurança pós-quântica, proporcionando proteção contra a ameaça de computadores quânticos. Utilizada para criptografar dados e garantir a autenticidade de assinaturas digitais, a criptografia baseada em redes é uma solução promissora para a segurança de informações no futuro.

ARTHUR GALASSI