Nome: Douglas Evangelista RA: 82516629

Atividade Aula 4

Exemplos Históricos

Códigos Navajo:

Durante a Segunda Guerra Mundial, os militares dos Estados Unidos utilizaram os códigos Navajo, que envolviam o uso da língua Navajo para transmitir mensagens confidenciais. A complexidade e a natureza não escritas da língua Navajo tornaram os códigos extremamente difíceis de serem decifrados pelos inimigos, proporcionando uma vantagem estratégica significativa aos Aliados.

Como Funcionava: Cifra Baseada na Língua: O código era uma combinação da língua navajo e substituições para palavras militares específicas. Por exemplo, a palavra "Águia" (na língua navajo, "Atsadi") representava o avião de combate (em inglês, "fighter plane"). Cada letra ou conceito seria traduzido por uma palavra navajo correspondente, mas com muitas palavras substituídas por outras de maneira codificada. Isso tornava as mensagens incompreensíveis para aqueles que não falavam navajo. Além disso, não existia um dicionário público do código, o que impedia os inimigos de decifrá-lo.

Scytale

A cifragem com o scytale (bastão, em grego) ou cítala espartana consiste em se enrolar uma fita de tecido em um bastão de madeira de dada largura. A frase a ser cifrada era escrita na fita no comprimento do bastão, densarolada e enviada disfarçada (como um cinto por exemplo) e ao chegar ao destino deveria ser enrolada num bastão de mesma largura para que a mensagem fosse decifrada.

Exemplo: Se você tiver um bastão de 3 colunas, a mensagem **"ENVIAR AS TROPAS"** seria escrita dessa maneira:

E N V

I A R

A S T

R O P

A S

Quando o papel é desenrolado, as letras ficam em uma ordem diferente: "EIAARNSVOTPS". Para decifrar a mensagem, é necessário usar um bastão do mesmo tamanho e enrolar o papel da mesma forma.

Algoritmos de criptografia com Chaves Simétricas utilizados atualmente

ChaCha20:

Algoritmo de criptografia simétrica que cifra e decifrar dados, como mensagens, e-mails e tráfego web. Foi desenvolvido por Daniel J. Bernstein, um criptologista e cientista da computação.

O ChaCha20 criptografa informações usando uma chave exclusiva e um nonce (um número usado apenas uma vez) para garantir que cada mensagem seja criptografada de forma diferente. Esse método torna extremamente difícil para os invasores descriptografar os dados sem a chave secreta. Sua eficácia se baseia no uso de rotações, adições e XOR (Operation Logic, Toggle, Cryptography), operações simples, mas poderosas, em criptografia.

Serpent:

Algoritmo de criptografia simétrica de bloco, projetado para ser uma alternativa segura ao DES e ao AES. participou da competição organizada pelo Instituto Nacional de Padrões e Tecnologia (NIST) para substituir o DES e se tornar o novo padrão de criptografia para o governo dos Estados Unidos, o AES. Embora o **Serpent** não tenha sido escolhido como o vencedor da competição ele é considerado um dos algoritmos de criptografia mais seguros e robustos.

A principal vantagem do Serpent é sua robustez e a segurança proporcionada pelas 32 rodadas e pela estrutura de criptografia forte e sua principal desvantagem é sua lentidão devidos ao número elevado de rodadas, isso pode ser um problema em dispositivos que precisam de criptografia de alta performance, como dispositivos móveis e sistemas de rede de alto desempenho.

Algoritmos de Criptografia com Chaves Assimétricas utilizados atualmente:

Kyber: O Kyber é fundamentado em problemas de redes matemáticas, mais especificamente no problema do vetor mais curto (SVP) e problemas de decodificação em redes. desenvolvido para ser resistente a ataques de computadores quânticos.

NTRU: é um algoritmo de criptografia assimétrica que se baseia em problemas de redes matemáticas. Ele foi projetado para ser eficiente em termos de tempo de

computação e memória, além de ser resistente a ataques de computadores quânticos

Tanto Kyber quanto NTRU foram desenvolvidos para substituir algoritmos tradicionais e garantir segurança contra possíveis ameaças através de computadores quânticos.