UC- SISTEMAS COMPUTACIONAIS E SEGURANÇA
Maria Eduarda Medeiro Porto 824144948
ORIENTADOR: Robson Calvetti

PRÁTICA 04- Proteção de Dados e Informação II

ATIVIDADE 1

Exemplos históricos de criptografia

Mary Stuart, Rainha da Escócia, e a Conspiração Babington (1586): Mary, Rainha da Escócia, usou um sistema criptográfico para se comunicar com seus co-conspiradores na Conspiração Babington, um plano para assassinar a Rainha Elizabeth I da Inglaterra. O sistema usava uma combinação de cifras de substituição e transposição para ocultar as mensagens. Embora a conspiração tenha sido finalmente descoberta, o uso de criptografia por Maria atrasou a detecção do complô.

O Telegrama Zimmermann (1917): Durante a Primeira Guerra Mundial, o Ministério das Relações Exteriores alemão usou um sistema criptográfico para enviar uma mensagem, conhecida como Telegrama Zimmermann, ao embaixador alemão no México. A mensagem, que foi interceptada e decifrada pela inteligência britânica, propôs uma aliança entre a Alemanha e o México contra os Estados Unidos. A decifração da mensagem contribuiu para a entrada dos Estados Unidos na guerra.

Algoritmos de Criptografia com Chaves Simétricas utilizados atualmente

AES (Advanced Encryption Standard): AES é um algoritmo de cifra de bloco de chave simétrica amplamente utilizado, considerado seguro e eficiente. É comumente usado para criptografar dados em repouso e em trânsito.

ChaCha20: ChaCha20 é uma cifra de fluxo projetada para ser rápida e segura. É frequentemente usada em protocolos como TLS e SSH.

Algoritmos de Criptografia com Chaves Assimétricas utilizados atualmente

RSA (Rivest-Shamir-Adleman): RSA é um algoritmo de chave assimétrica amplamente utilizado que é comumente usado para transmissão segura de dados, assinaturas digitais e autenticação.

ECDSA (Elliptic Curve Digital Signature Algorithm): ECDSA é um tipo de algoritmo de chave assimétrica que é usado para assinaturas digitais e autenticação. É comumente usado em criptomoedas como Bitcoin e Ethereum.