Paulo Henrique Luiz do Monte

RA: 82325475

Atividade 3

1. Exemplos históricos do uso de criptografia

Cifra de Políbio (Grécia Antiga, Século II a.C.): Desenvolvida pelo historiador grego Políbio, esta cifra é um dos primeiros exemplos de substituição. O método consistia em uma tabela 5x5 (Quadrado de Políbio) onde as letras do alfabeto eram dispostas. Cada letra era substituída pelas coordenadas de sua posição na tabela. Foi utilizada principalmente para telegrafia e sinalização a longas distâncias.

Disco de Alberti (Renascença, Século XV): Criado pelo humanista italiano Leon Battista Alberti, é considerado o primeiro dispositivo de cifra polialfabética. Consistia em dois discos concêntricos, um fixo e outro móvel, que permitiam mudar a correspondência entre as letras durante a mensagem. Tornava a análise de frequência muito mais difícil, sendo precursor de sistemas mais complexos como a máquina Enigma.

Cifra da Escítala (Esparta, Século V a.C.): Utilizava tiras de couro enroladas em um bastão de diâmetro específico. A mensagem só podia ser lida corretamente ao ser enrolada no bastão correspondente. Foi um dos primeiros métodos de transposição.

Máquina Enigma (Alemanha, Segunda Guerra Mundial): Máquina eletromecânica que produzia cifras complexas através de rotores. Teve grande impacto histórico, pois sua quebra pelos Aliados foi decisiva para encurtar a guerra, marcando a transição da criptografia manual para a mecânica.

2. Algoritmos de criptografia com chaves simétricas utilizados atualmente

AES (Advanced Encryption Standard): Padrão internacional de criptografia, usado em comunicações seguras na internet, proteção de dados em discos e segurança de redes Wi-Fi. Opera com blocos de 128 bits e chaves de 128, 192 ou 256 bits.

ChaCha20-Poly1305: Algoritmo moderno de fluxo, adotado em conexões HTTPS como substituto do RC4. Combina a cifra ChaCha20 com o autenticador Poly1305, garantindo confidencialidade, integridade e autenticidade.

3. Algoritmos de criptografia com chaves assimétricas utilizados atualmente

RSA (Rivest-Shamir-Adleman): Baseado na dificuldade de fatorar grandes números. Utilizado em assinaturas digitais e na troca segura de chaves em protocolos como o HTTPS.

ECC (Elliptic Curve Cryptography): Baseada em curvas elípticas, garante a mesma segurança que o RSA com chaves menores, sendo mais eficiente. É aplicada em dispositivos móveis, cartões inteligentes e criptomoedas.

Diffie-Hellman: Um dos primeiros métodos de troca de chaves públicas. Ainda hoje é base de protocolos como o TLS.

DSA (Digital Signature Algorithm): Algoritmo voltado para assinaturas digitais, bastante empregado em sistemas oficiais e governamentais.

4. Complemento

A criptografia evoluiu de métodos manuais simples, como o Quadrado de Políbio, até dispositivos mecânicos, como a Enigma, e hoje alcança algoritmos matemáticos altamente sofisticados, como o AES e a ECC. Atualmente, é fundamental para a segurança digital, permitindo desde o uso de bancos online até a comunicação segura em aplicativos de mensagens e transações financeiras.