Victor Domingos Moreira - 825155879

Felipe Duarte Battaglini - 825165863

Cauã Guidio Viana - 825168423

Lucas Gonçalves da Silva-825113362

Victor de Morais Nelson 825243925

Histórico da Criptografia

Em vez de focar nas cifras mais comuns, como a Cifra de César, estes dois exemplos mostram a engenhosidade humana em proteger mensagens ao longo da história:

A Cítala Espartana (c. 650 a.C.): Este é um dos exemplos mais antigos de criptografia por transposição, onde a ordem das letras é alterada. A mensagem era escrita em uma tira de couro que era enrolada em um bastão cilíndrico (a cítala). O segredo para decifrar a mensagem — a chave — era o diâmetro exato do bastão. Se o bastão tivesse o tamanho errado, a mensagem parecia um amontoado de letras sem sentido. Era crucial para a comunicação militar espartana.

O Cifrário de Vigenère (Século XVI): Apelidado de "a cifra indestrutível" na época, é um exemplo de cifra polialfabética. Ao contrário de cifras simples que usam apenas um deslocamento fixo para todo o texto, Vigenère usa uma palavra-chave para aplicar diferentes deslocamentos a cada letra. Essa técnica esconde a frequência real das letras, o que a tornou extremamente resistente à análise de frequência, que era o principal método de quebra de códigos da época.

Criptografia com Chaves Simétricas (Atualidade)

A criptografia simétrica é a mais rápida. Ela utiliza uma única chave secreta tanto para cifrar quanto para decifrar os dados.

AES (Advanced Encryption Standard): É considerado o padrão de criptografia mais utilizado no mundo e é a escolha do governo dos EUA para proteger informações classificadas. Ele usa chaves de 128, 192 ou 256 bits. O AES é fundamental em praticamente tudo o que fazemos hoje, desde a criptografia de disco rígido (como BitLocker) até a proteção de redes Wi-Fi (WPA2/WPA3).

ChaCha20: É um algoritmo de cifra de fluxo mais recente, conhecido por sua extrema velocidade e segurança. Desenvolvido para superar o desempenho do AES em software, ele é particularmente eficiente em dispositivos móveis e sistemas de baixo consumo. Por isso, é amplamente adotado em protocolos modernos, como o TLS 1.3, para acelerar a comunicação segura na web.

Criptografia com Chaves Assimétricas (Atualidade)

A criptografia assimétrica (ou de chave pública) utiliza um par de chaves interligadas: uma chave pública (que pode ser compartilhada) e uma chave privada (que deve ser mantida em segredo).

RSA (Rivest, Shamir e Adleman): É o algoritmo de chave pública mais popular e amplamente usado desde o final dos anos 70. Sua segurança se baseia na dificuldade matemática de fatorar números primos muito grandes. O RSA é a espinha dorsal dos certificados digitais (SSL/TLS), sendo usado para a troca segura de chaves simétricas e para assinaturas digitais (garantindo que o remetente é quem diz ser).

ECC (Elliptic Curve Cryptography): É um sistema mais moderno e eficiente que o RSA. Sua segurança se baseia em cálculos complexos em curvas elípticas. A grande vantagem é que o ECC atinge o mesmo nível de segurança que o RSA, mas com chaves muito menores. Por exemplo, uma chave ECC de 256 bits oferece segurança comparável a uma chave RSA de 3072 bits. Isso o torna ideal para dispositivos com processamento limitado, como smartphones e tablets.