FACULDADE SÃO JUDAS TADEU

SISTEMAS COMPUTACIONAIS E SEGURANÇA

ALUNO:

BOAZ MOREIRA CIRINO - RA: 825146412

EXEMPLOS HISTÓRICOS DO USO DE CRIPTOGRAFIA E ALGORITMOS DE CRIPTOGRAFIA

SÃO PAULO  
2025

Criptografia:

A criptografia está mais presente no cotidiano nosso do que se imagina. Assinatura digital, privacidade de dados e muito mais dependem dela

Despercebida, a criptografia está mais presente no cotidiano das pessoas do que se imagina. Para se ter uma ideia, atualmente, diversos serviços públicos do governo federal ofertados digitalmente utilizam a tecnologia, como sites e aplicativos móveis de serviços públicos, inclusive do Brasil.

No país, os agentes do governo entendem que a criptografia é uma técnica milenar de proteção de dados, que evoluiu ao longo do tempo e é atualmente um importante mecanismo de segurança da informação.

Exemplos históricos do uso de criptografia:

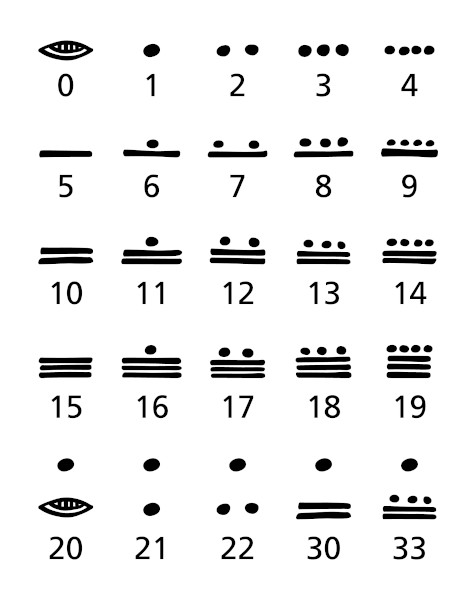
**Cifras Maias (Civilização Maia, Século IX):**

O sistema de numeração maia é a estrutura de contagem e representação numérica adotada pela civilização pré-colombiana maia. Utilizando pontos, traços e conchas, os maias escreviam os números considerando uma base vigesimal.

**Quais são as características do sistema de numeração maia?**

O sistema de numeração maia utilizava três símbolos para escrever os números: uma concha, um ponto e um traço horizontal. A concha possuía o mesmo significado que o número 0 no nosso sistema de numeração, como veremos adiante. Já o ponto indicava a unidade e o traço, o número cinco.

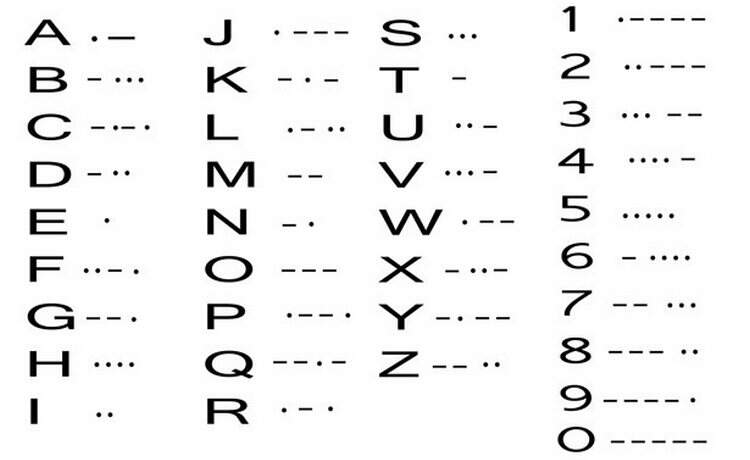
A base adotada no sistema de numeração maia era vigesimal, ou seja, de base 20. Isso significa que os conjuntos de símbolos utilizados na escrita de um número estavam associados a potências de 20.



**Código Morse Secreto (Guerra do Vietnã, 1966):**

O Código Morse é um método de comunicação que representa letras, números e pontuação através de uma sequência de pontos e traços, criando uma mensagem codificada que é enviada de modo intermitente. Esse sistema permite a transmissão de mensagens à distância por fio ou via rádio, através de sons de curta e de longa duração.

A comunicação através do Código Morse pode ser feita de diferentes formas. A transmissão das mensagens codificadas em Morse pode ser feita por pulsos elétricos, por meio de uma rede telegráfica; por ondas mecânicas, através do som; por ondas eletromagnéticas, através de sinais de rádio com pulsos ou tons curtos e longos; ou ainda, por sinais visuais, utilizando ferramentas como lâmpadas e heliógrafos.



Algoritmos de criptografia com chaves simétricas:

**AES (Advanced Encryption Standard)**

O AES funciona convertendo texto simples (plaintext) em texto cifrado (ciphertext) usando uma abordagem de cifra de bloco. Ele opera com blocos de dados de tamanho fixo (128 bits) e suporta três comprimentos de chave: 128, 192 ou 256 bits. Quanto maior o comprimento da chave, mais forte é a criptografia. O algoritmo emprega uma série de operações de substituição, permutação e mistura em várias rodadas para garantir a segurança dos dados.

**ChaCha20**

O algoritmo funciona gerando uma sequência de números pseudoaleatórios, chamada de fluxo de chave, que é combinada com os dados originais para produzir o texto cifrado. ChaCha20 utiliza uma chave de 256 bits e um contador de 64 bits para oferecer alta segurança, e sua estrutura é projetada para resistir a ataques criptográficos conhecidos.

Algoritmos de criptografia com chaves asimétricas:

**RSA (Rivest-Shamir-Adleman)**

No RSA, a chave pública é usada para criptografar informações, enquanto a chave privada é usada para descriptografá-las. Isso permite comunicação segura, já que somente o destinatário que possui a chave privada pode acessar os dados enviados com a chave pública. O algoritmo baseia-se em conceitos matemáticos relacionados à fatoração de números grandes, o que garante sua segurança: quebrá-lo requer uma enorme quantidade de poder computacional.

**ECC (Elliptic Curve Cryptography)**

A principal vantagem da ECC é sua eficiência: com chaves menores, ela oferece o mesmo nível de segurança de métodos que utilizam chaves maiores, como RSA. Por exemplo, uma chave ECC de 256 bits é considerada tão segura quanto uma chave RSA de 3072 bits. Isso a torna ideal para dispositivos com recursos limitados, como smartphones, IoT (Internet das Coisas) e sensores.

Bibliografias:

RIZZO, M. L. A. **Sistema de numeração maia**. Disponível em: <https://mundoeducacao.uol.com.br/matematica/o-sistema-numeracao-maia.htm>. Acesso em: 24 mar. 2025.

TUPINAMBÁ, R. **A história da criptografia**. Disponível em: <https://cryptoid.com.br/identidade-digital-destaques/a-historia-da-criptografia-2/>. Acesso em: 24 mar. 2025.

BRASIL, E. M. **Educa Mais Brasil - Bolsas de Estudo de até 70% para Faculdades – Graduação e Pós-graduação**. Disponível em: <https://www.educamaisbrasil.com.br/enem/lingua-portuguesa/codigo-morse>. Acesso em: 24 mar. 2025.