



Simétricas/Assimétricas

03/04

CRIPTO- GRAFIA



www.criptografia.com





EXEMPLOS HISTÓRICOS DO USO DA CRIPTOGRAFIA

03/04

- **Cifra de Escítala (Grécia Antiga)**

Usada pelos espartanos para comunicação militar secreta durante o período das Guerras do Peloponeso.

Consistia em um bastão cilíndrico onde uma tira de couro ou papiro era enrolada. Quando desenrolada, a mensagem parecia uma sequência aleatória de letras. Apenas quem possuía um bastão com o mesmo diâmetro conseguia alinhar corretamente o texto e ler a mensagem.

Esse método foi um dos primeiros exemplos de criptografia transpositiva.



www.criptografia.com



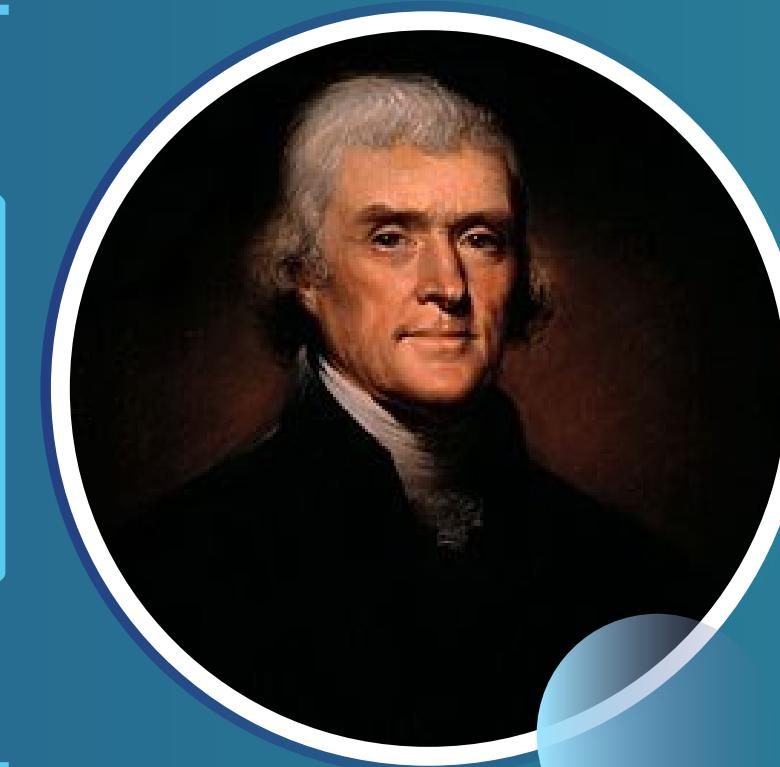


CIFRA DE JEFFERSON (RODA DE CIFRAS, SÉCULO XVIII)

03/04



Criada por Thomas Jefferson no final do século XVIII, a Roda de Cifras era composta por 36 discos de madeira empilháveis, cada um contendo o alfabeto disposto de forma aleatória. Para codificar uma mensagem, os discos eram girados até alinhar o texto original em uma das linhas, e uma das linhas alternativas servia como o texto cifrado. Esse método foi redescoberto e adotado pelos militares americanos no século XX, sendo usado em diversas operações estratégicas.



www.criptografia.com





AES (Advanced Encryption Standard)

O AES foi criado pelo Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) no final dos anos 1990 como um substituto do DES (Data Encryption Standard).

Utiliza tamanhos de chave de 128, 192 ou 256 bits, sendo altamente seguro e eficiente para diversas aplicações.

É amplamente empregado para a proteção de dados em redes sem fio, bancos de dados, transações bancárias e dispositivos móveis.

ALGORITMOS DE CRIPTOGRAFIA COM CHAVES SIMÉTRICAS





Blowfish

Desenvolvido por Bruce Schneier em 1993, o Blowfish é um algoritmo de chave simétrica que oferece velocidade e flexibilidade.

Utiliza chaves variáveis de 32 a 448 bits e um mecanismo de substituição e permutação para tornar o ataque por força bruta extremamente difícil.

É comumente usado em softwares de criptografia de senhas e na proteção de redes privadas virtuais (VPNs).

ALGORITMOS DE CRIPTOGRAFIA COM CHAVES SIMÉTRICAS





ALGORITMOS DE CRIPTOGRAFIA COM CHAVES ASSIMÉTRICAS

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

Desenvolvido em 1977 por Ron Rivest, Adi Shamir e Leonard Adleman, o RSA é um dos algoritmos de criptografia assimétrica mais amplamente utilizados.

Baseia-se na dificuldade de fatorar números primos muito grandes, tornando sua segurança extremamente robusta.

É amplamente aplicado em protocolos de comunicação segura, como SSL/TLS, assinatura digital e criptografia de e-mails.





ALGORITMOS DE CRIPTOGRAFIA COM CHAVES ASSIMÉTRICAS

- **ECC (Elliptic Curve Cryptography)**

A criptografia de curva elíptica (ECC) é um método moderno que oferece um alto nível de segurança com chaves menores do que o RSA. Utiliza propriedades matemáticas de curvas elípticas sobre corpos finitos para criar sistemas criptográficos altamente eficientes. É especialmente útil para dispositivos móveis, sistemas embarcados e Internet das Coisas (IoT), onde a eficiência energética e o baixo uso de processamento são cruciais.





Simétricas/Assimétricas

03/04

OBRIGADO PELA ATENÇÃO!



www.criptografia.com

