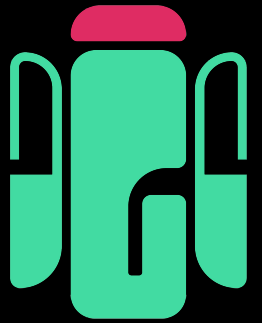
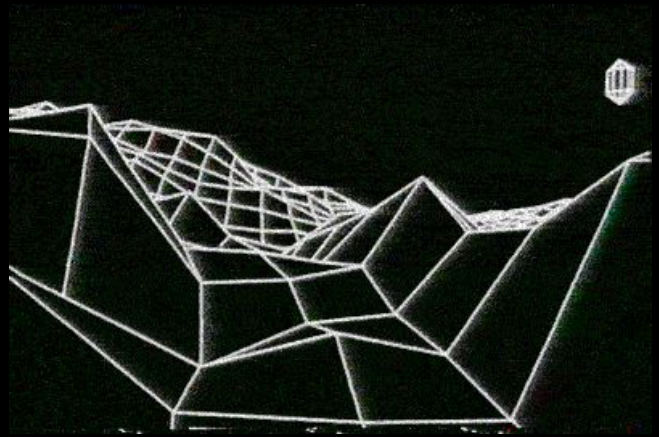
Criptografia

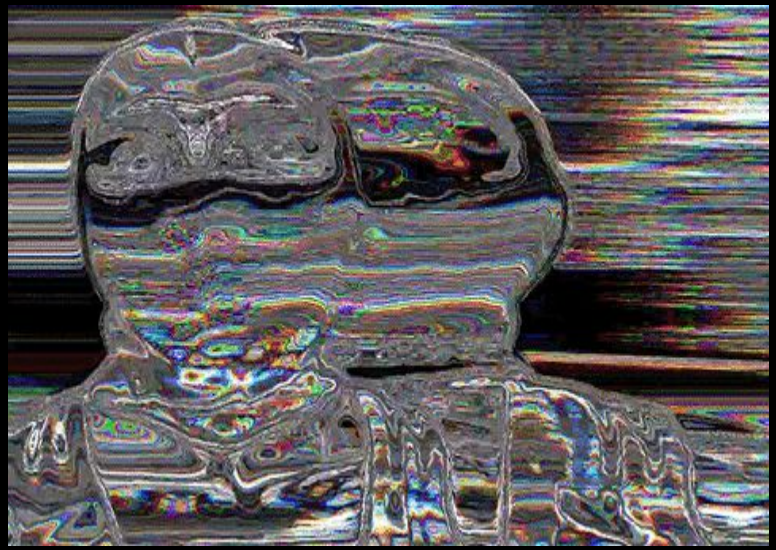


objetivos da criptografia



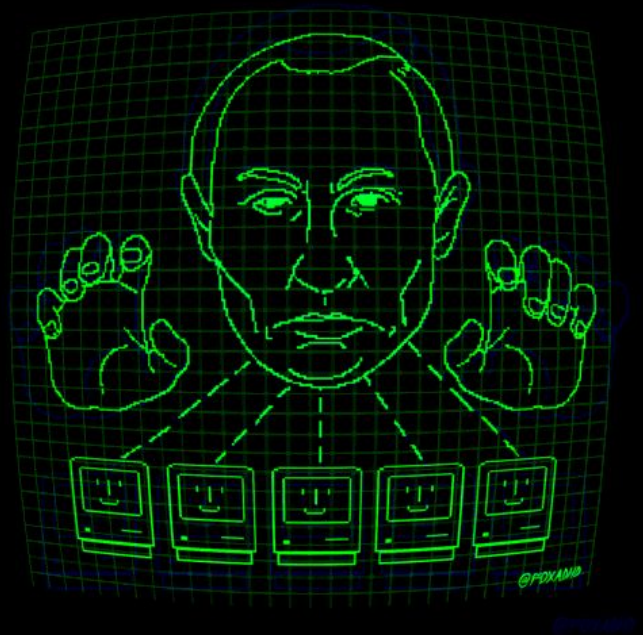
confidencialidade

a informação não pode ser entendida por ninguém que não seja o remetente



autenticação

o remetente e o destinatário conseguem confirmar a identidade do outro e a origem/destino da informação



integridade

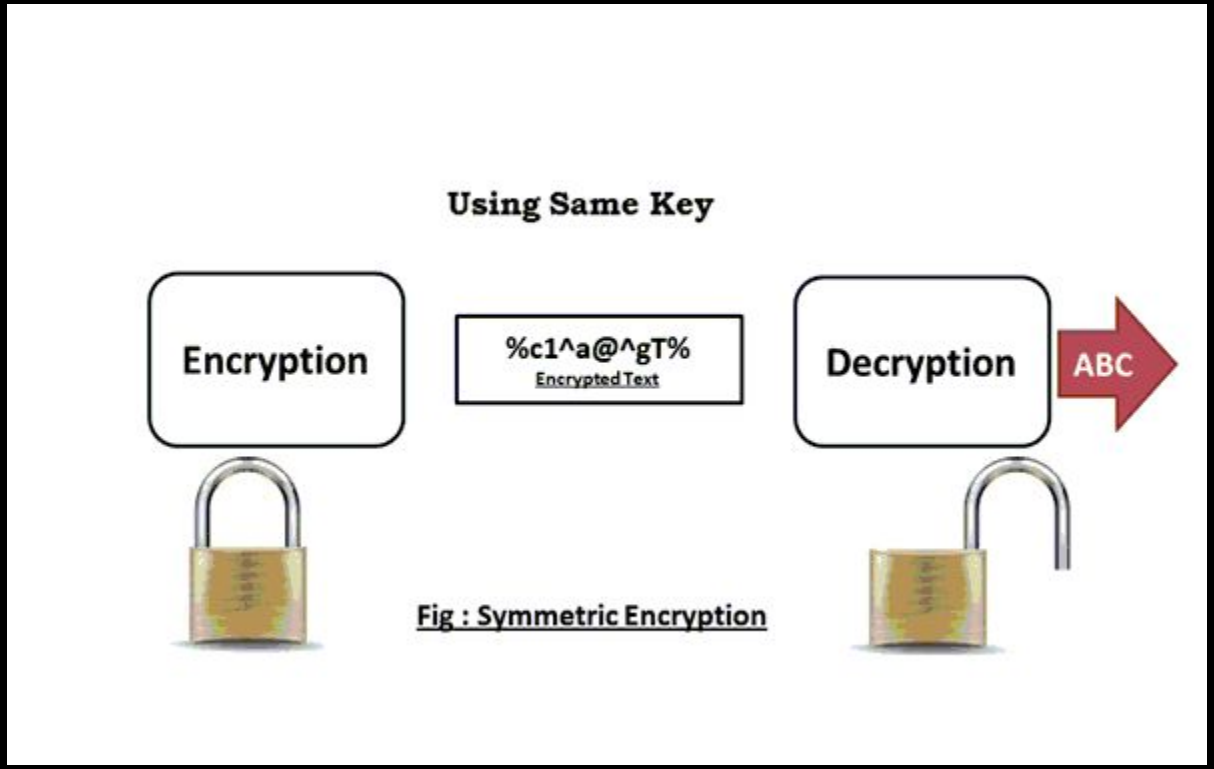
a informação não pode ser alterada no armazenamento nem no trânsito entre o remetente e o destinatário

2 Tipos de tratamentos da informação

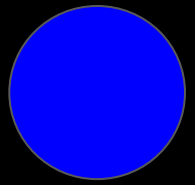
Encriptar

Desencriptar

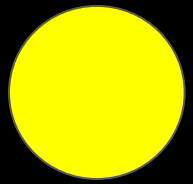
Criptografia Simétrica



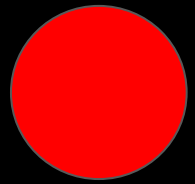
chave

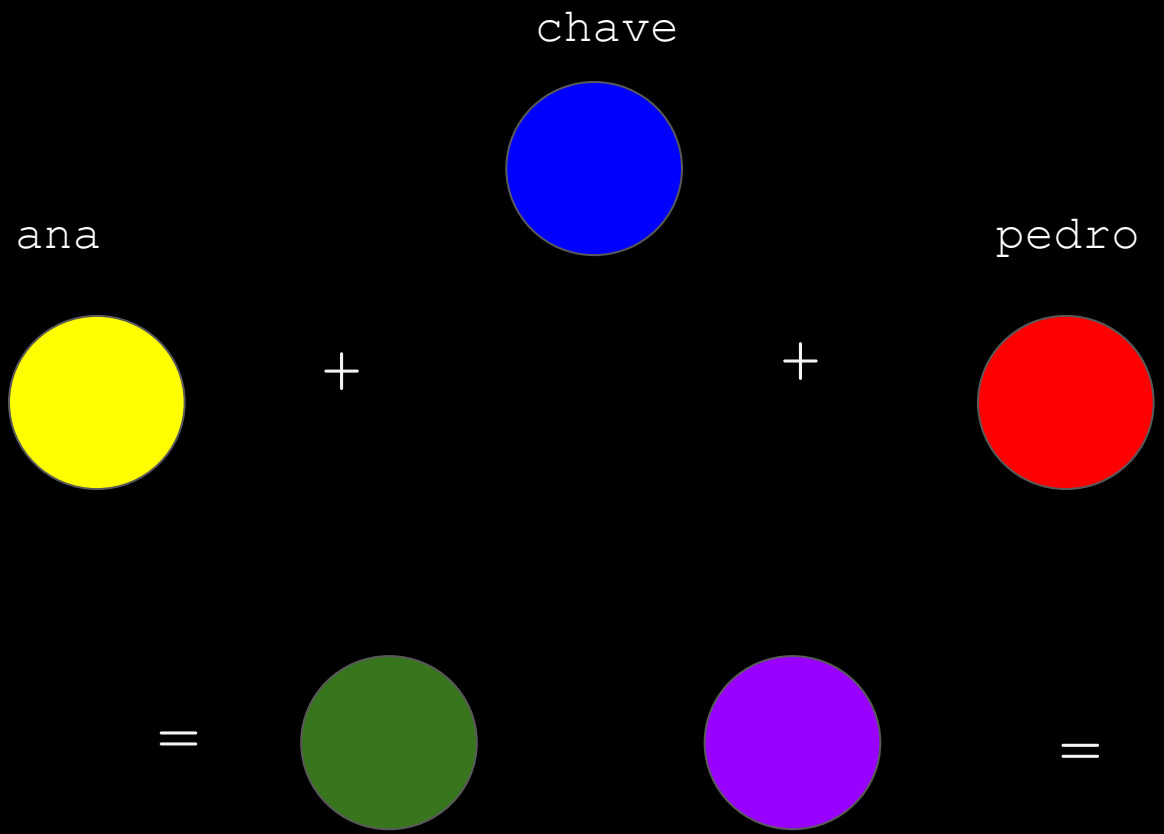


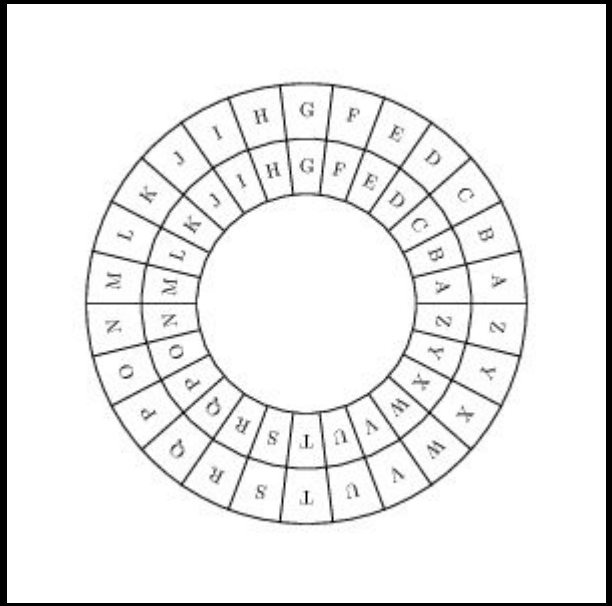
ana



pedro




chave
ana
pedro
+
+
=
=



Tipos clássicos de criptografia

caesar cipher

vigenère cipher


11011001
01011010
11010110.

Criptografia Assimétrica

- chaves públicas

  criptografia

- chaves privadas

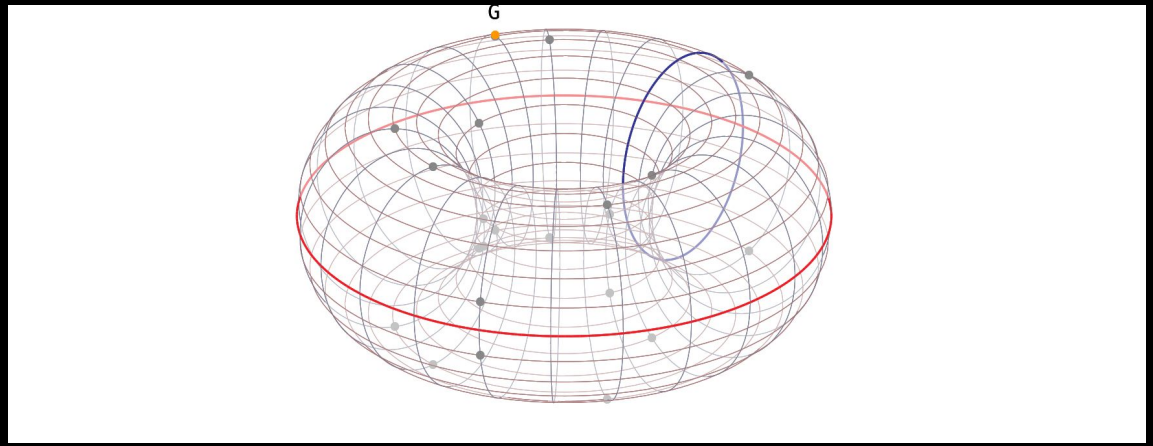
  descriptografia

  ex: RSA

RSA (Rivest-Shamir-Adleman)

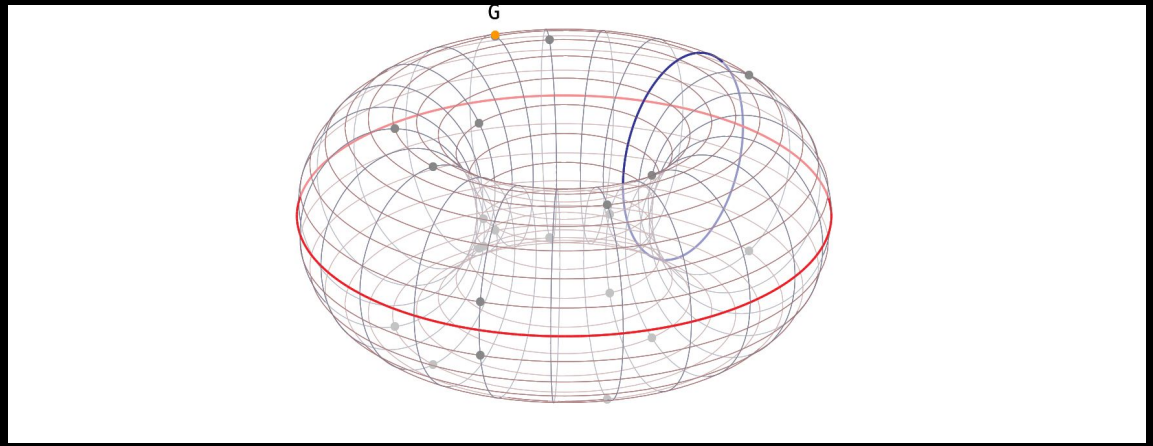
- Um dos primeiros algoritmos a usar chaves públicas
- Utiliza-se da dificuldade matemática de calcular logaritmos discretos

Curvas Elípticas



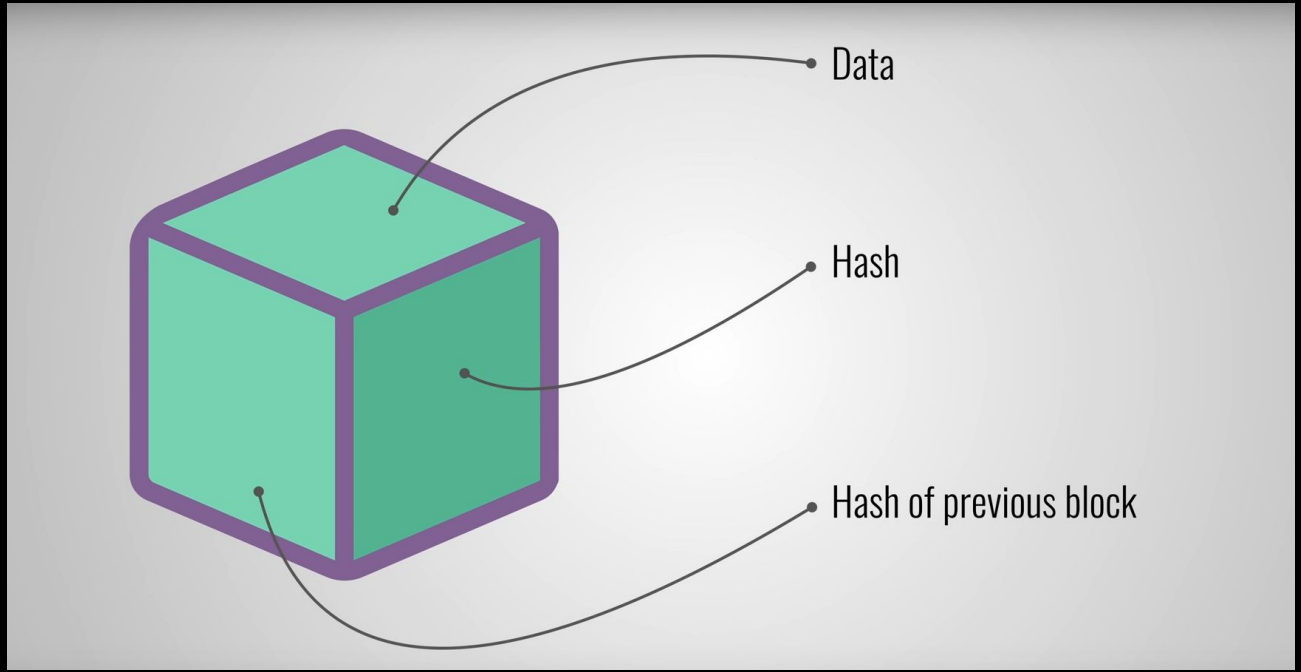
Curvas Elípticas

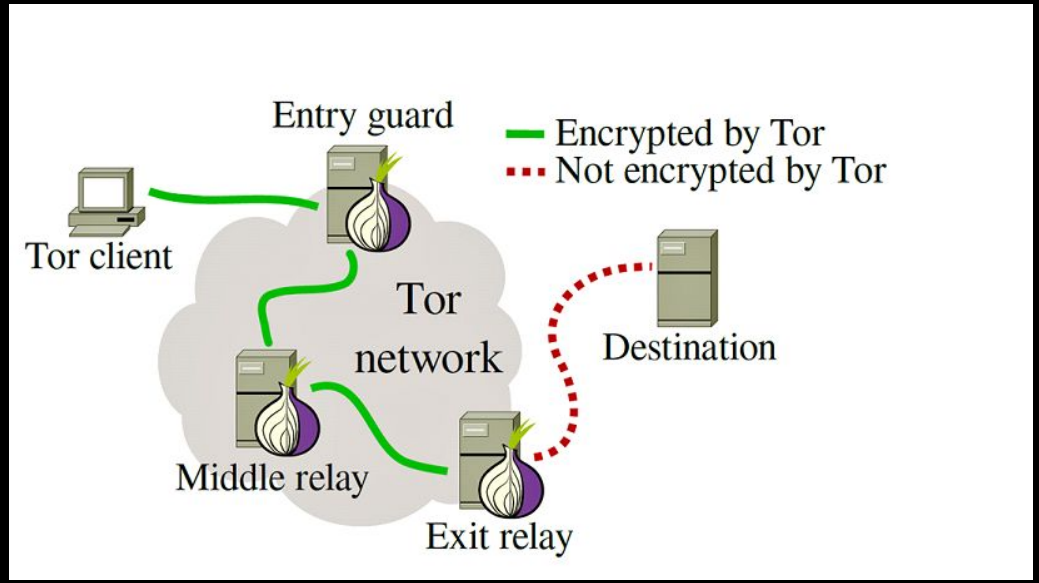
Curvas Elípticas



Criptomoedas


HOW BLOCKCHAIN WORKS:
BIT.LY/ADTECHGIFS


Data
Hash
Hash of previous block


Entry guard
Encrypted by Tor
Not encrypted by Tor
Tor client
Tor
network
Destination
Middle relay
Exit relay


NÃO HÁ LIBERDADE SEM PRIVACIDADE
NO HAY LIBERTAD SIN PRIVACIDAD
THERE IS NO FREEDOM WITHOUT PRIVACY
IL N'Y A PAS LA LIBERTÉ SANS VIE PRIVÉE