Criptografia 101

Eduardo Mendes
github.com/z4r4tu5tr4

z4r4tu5tr4@babbge: screenfetch

Nome: Eduardo Mendes
Instituição: Fatec Americana
Uptime: 12097080s
Email: mendexeduardo@gmail.com
git: github.com/z4r4tu5tr4

- Teoria da “comunicação”
- Cifras de rotação
- Sistemas distribuídos
- Cifras assimétricas
- Cifras simétricas
- Hash

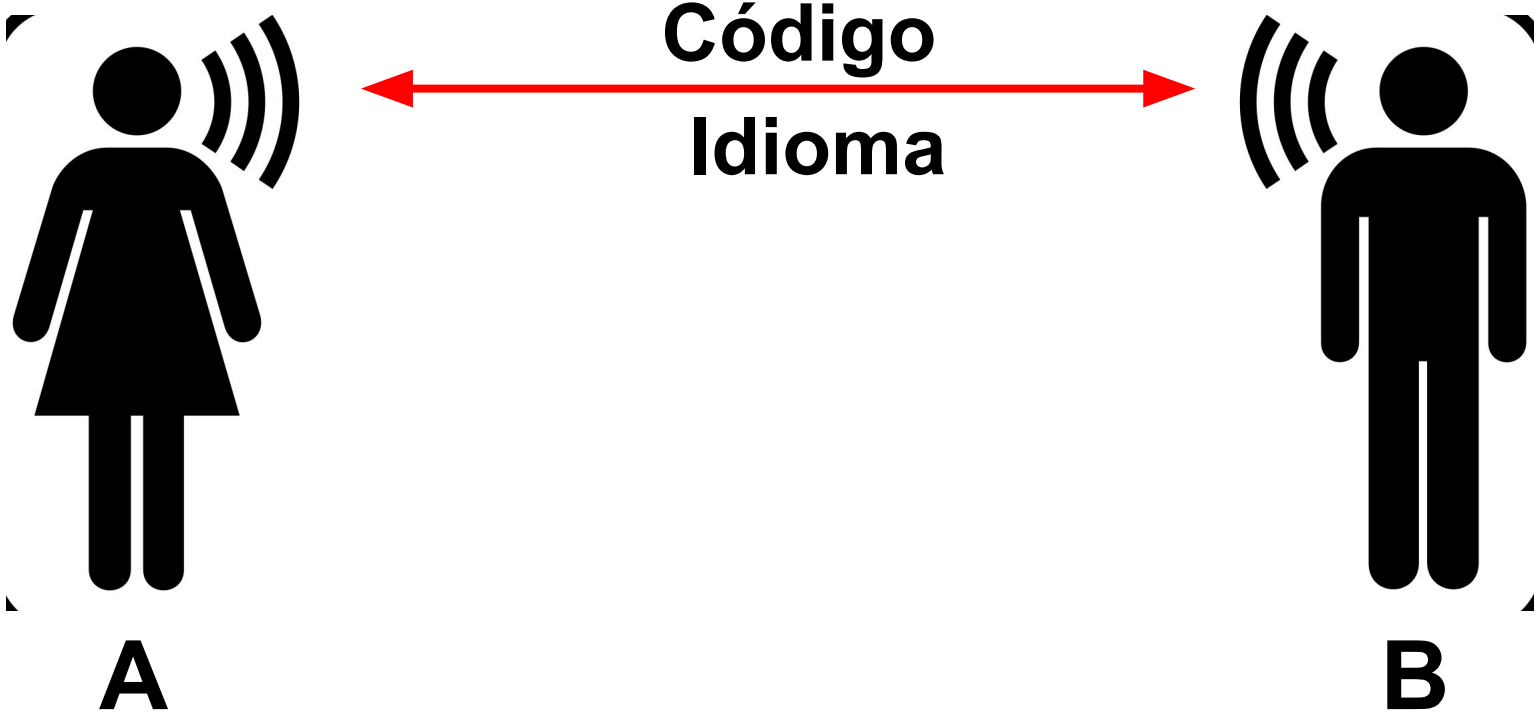
Estrutura

Teoria da “comunicação”

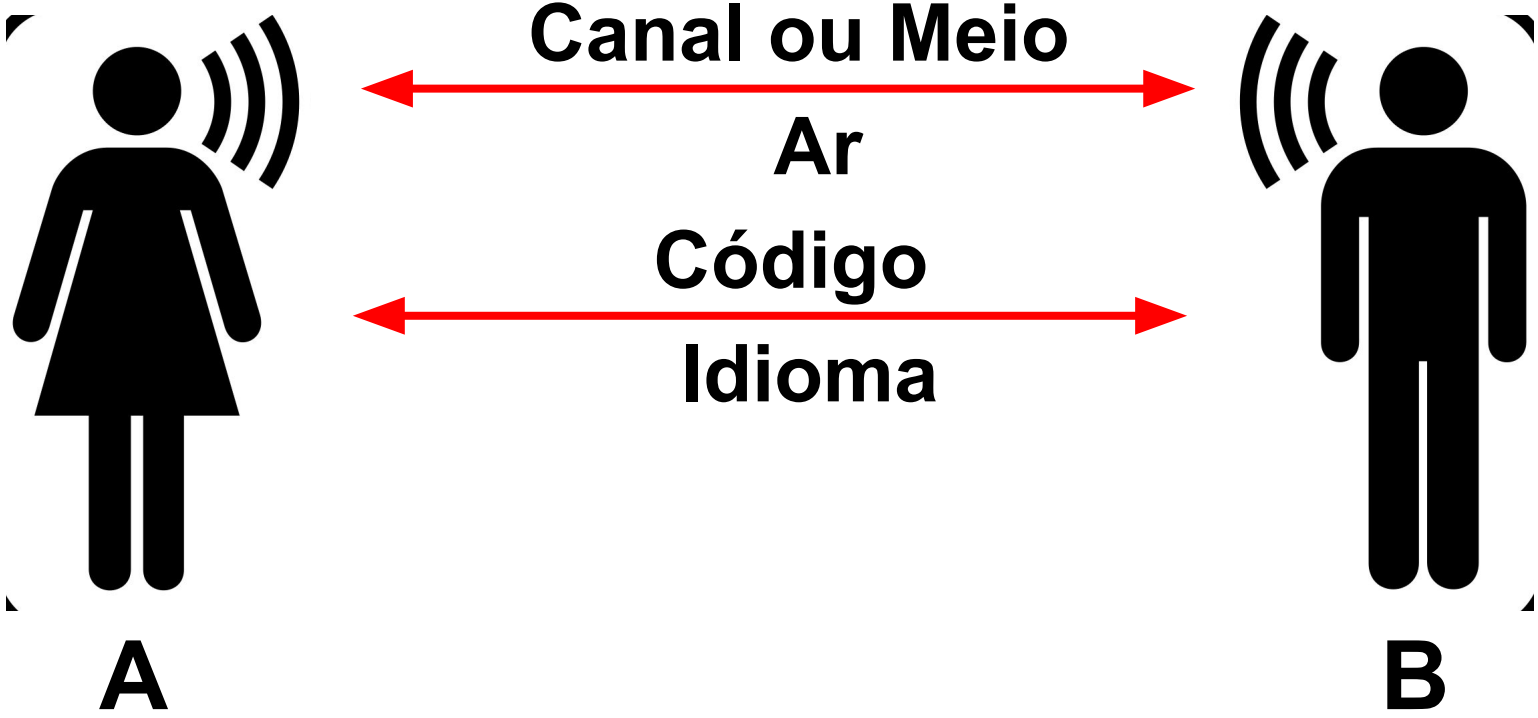
O básico e simples

Como funciona a comunicação verbal? [0]

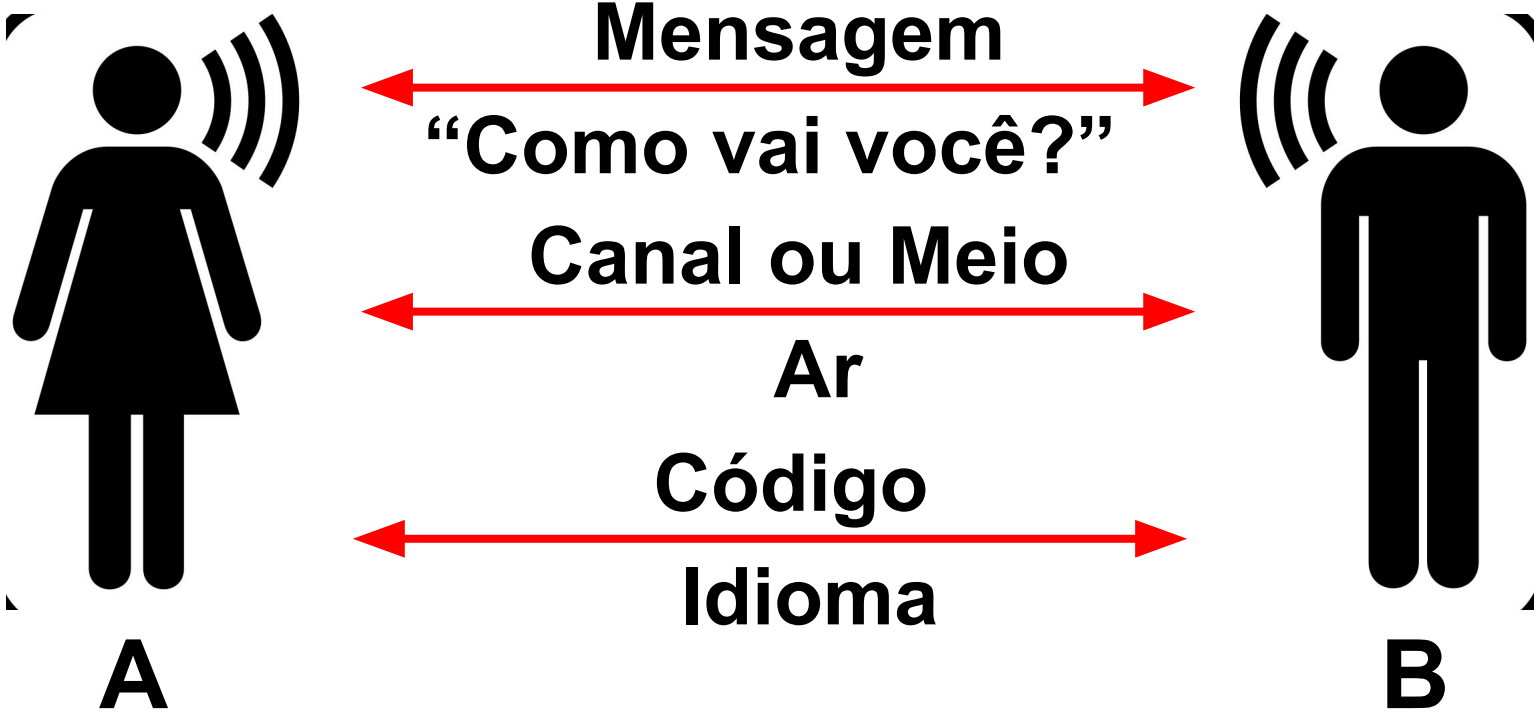
Como funciona a comunicação verbal? [1]



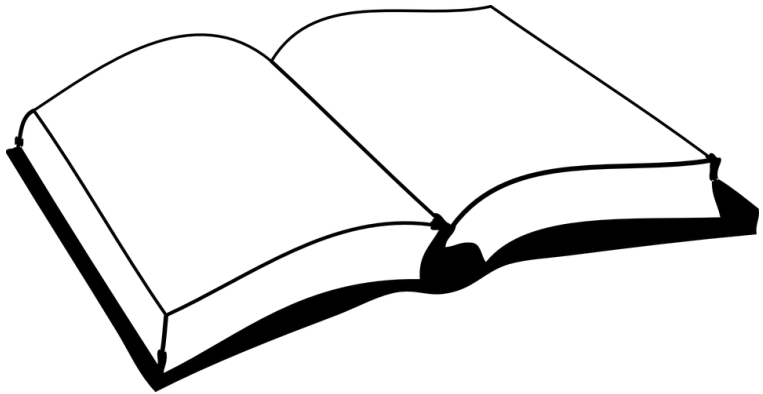
Como funciona a comunicação verbal? [2]



Como funciona a comunicação verbal? [3]

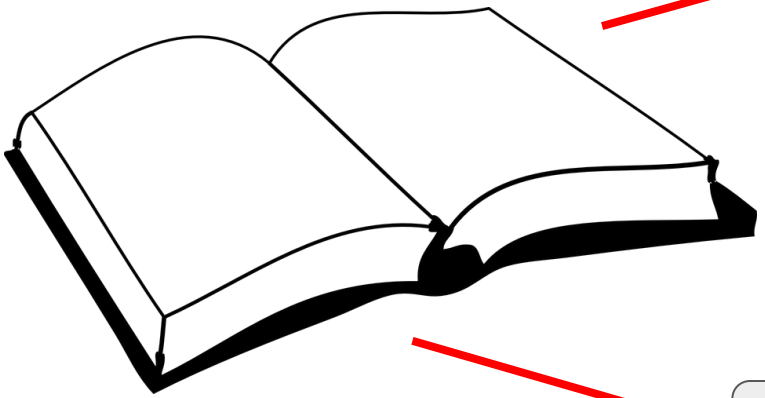


E a comunicação escrita? [0]



?

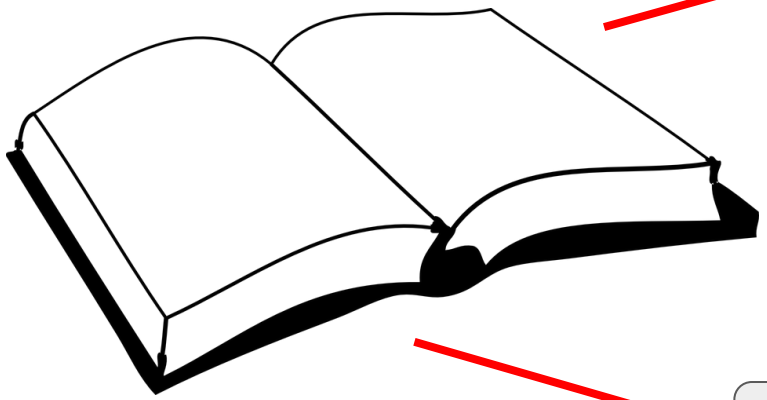
E a comunicação escrita? [1]



Separa o emissor do receptor

Altera o canal

E a comunicação escrita? [2]



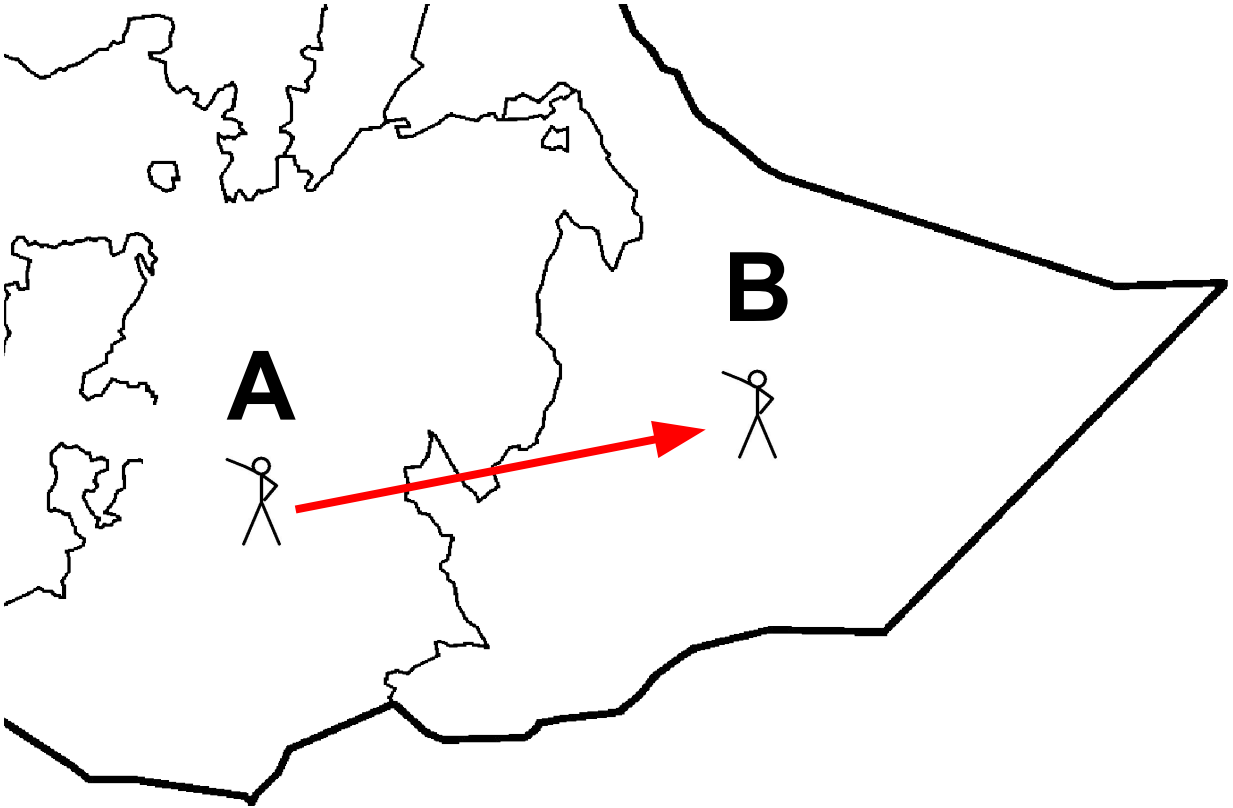
Separa o emissor do receptor

Tempo

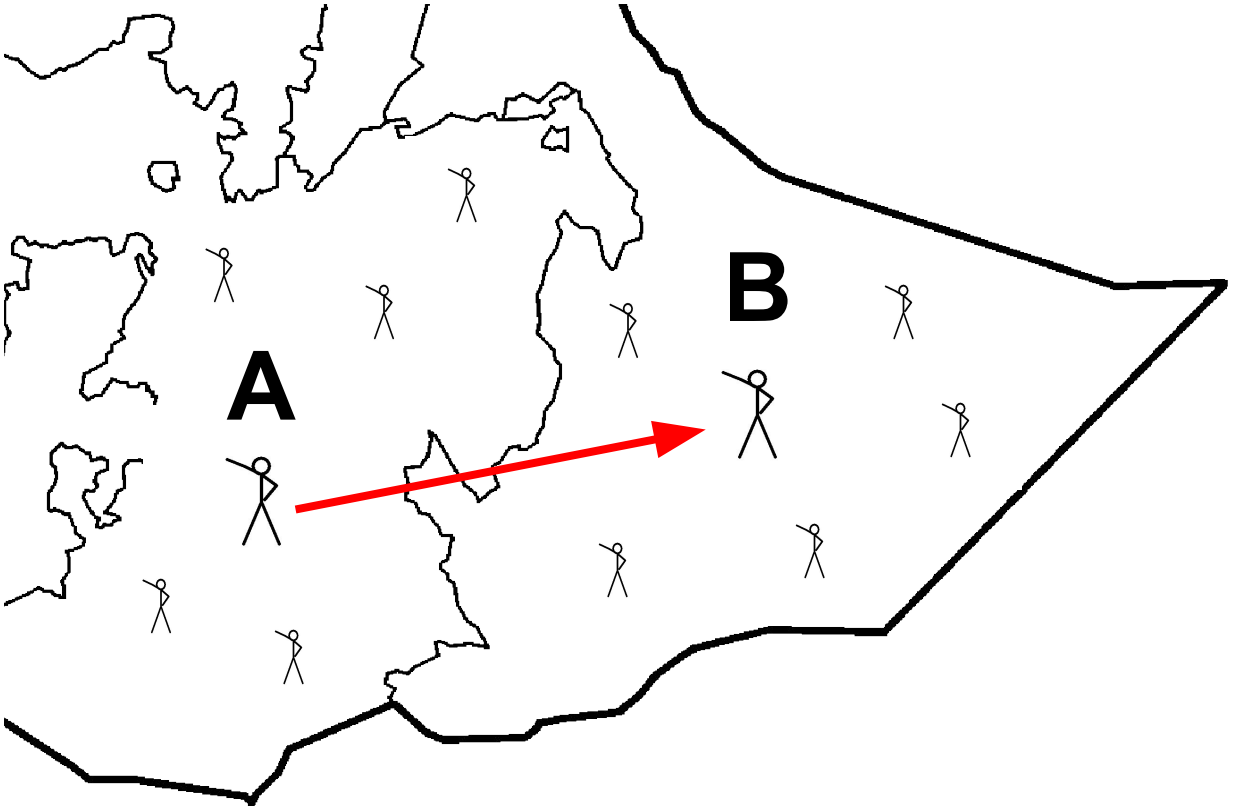
Espaço

Altera o canal

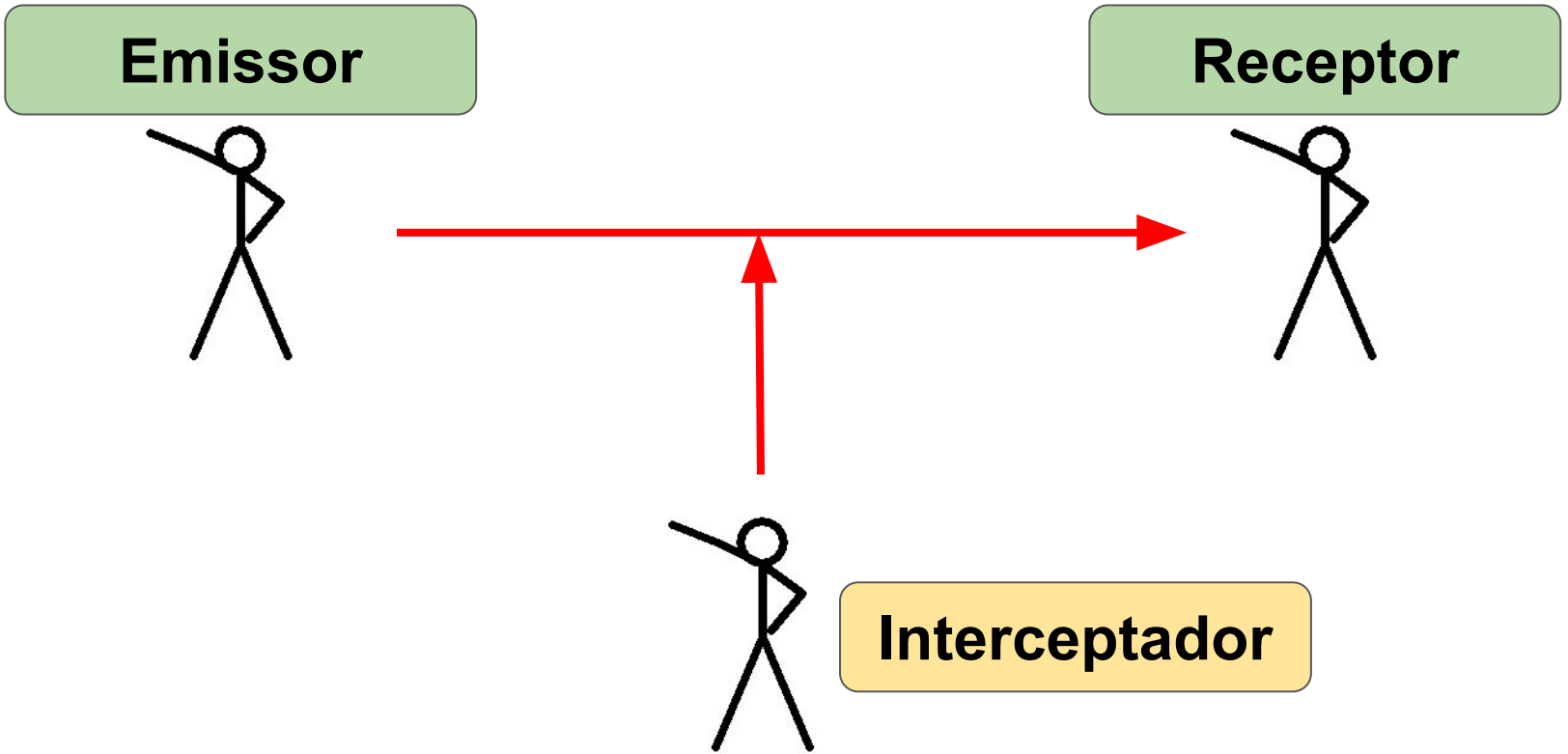
Transporte de informação [0]



Transporte de informação [1]



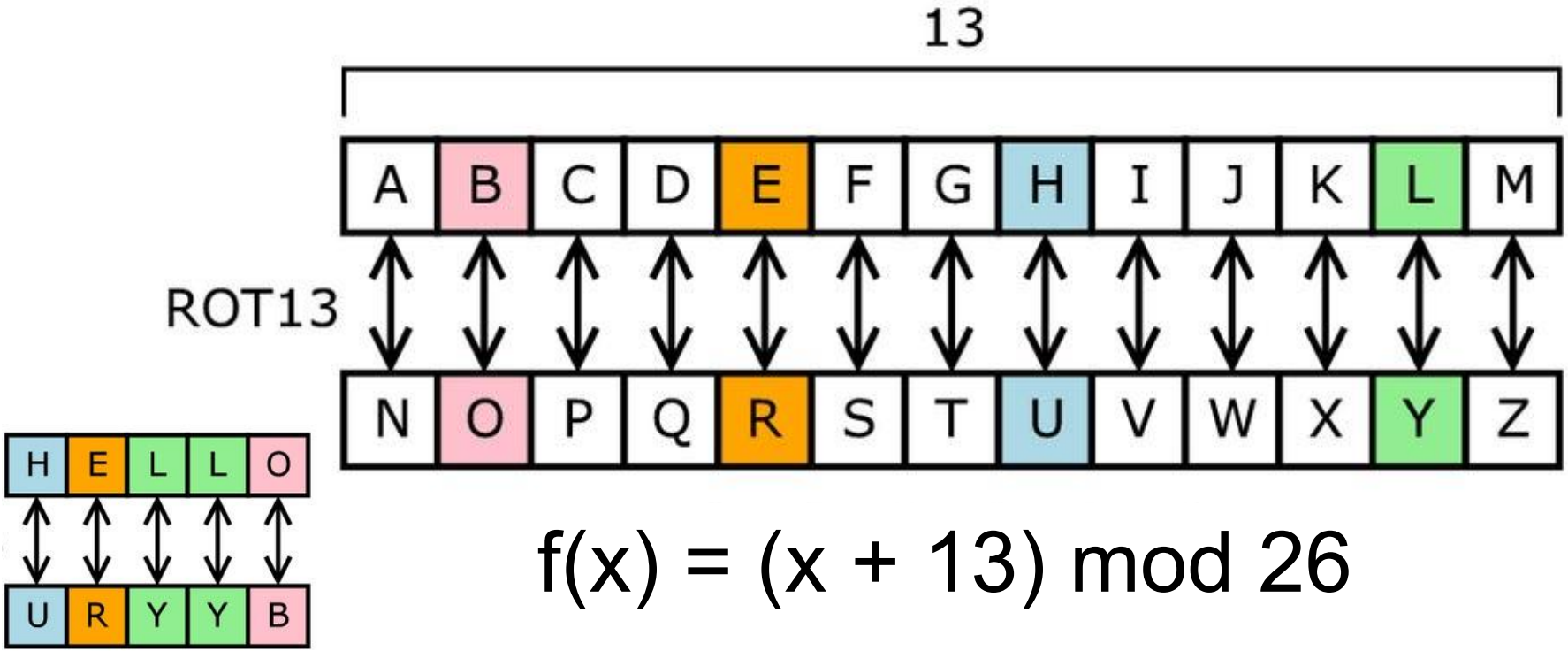
Transporte de informação [2]



Cifras de rotação

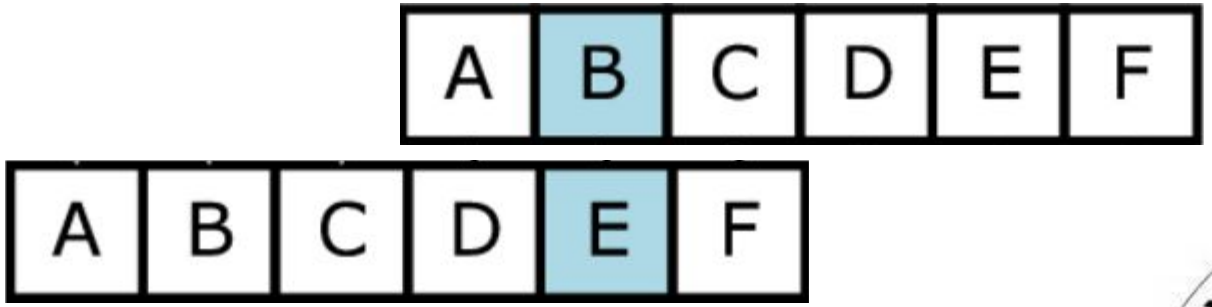
O começo de tudo

Cifra de rotação [0]



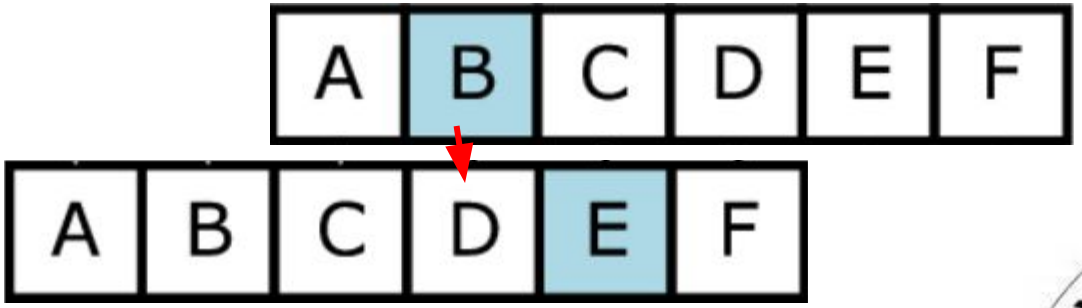
$$f(x) = (x + 13) \bmod 26$$

Cifra de rotação [1]



$$f(x) = (x + 3) \bmod 26$$

Cifra de rotação [2]



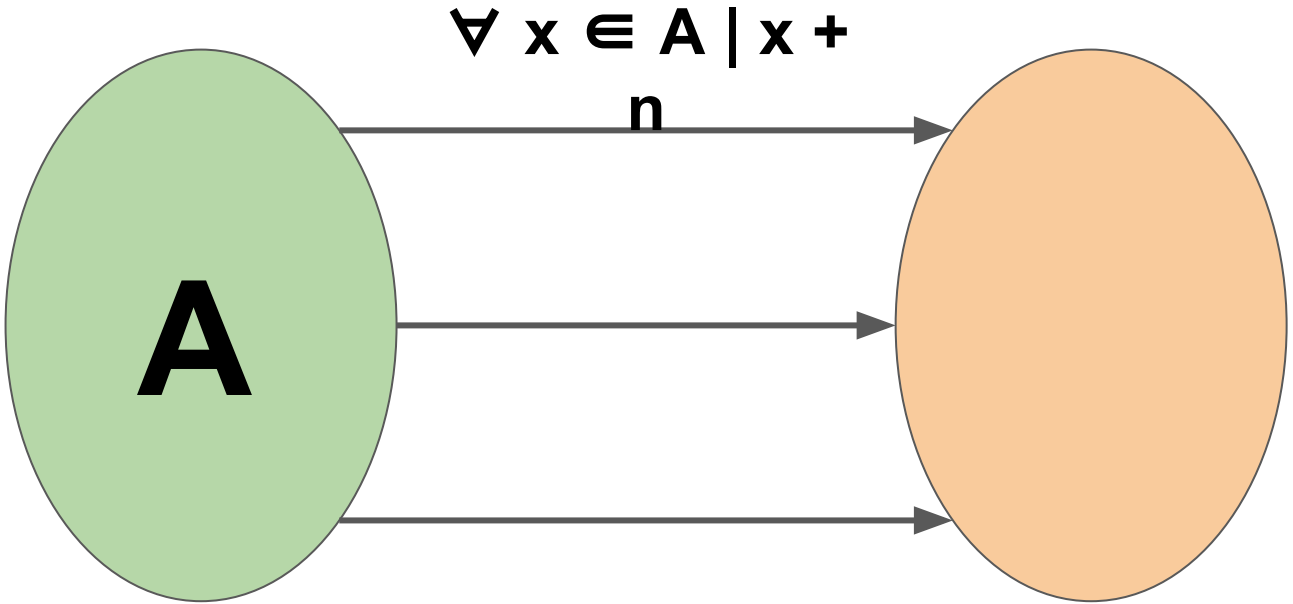
$$f(x) = (x + \mathbf{2}) \bmod 26$$

Cifra de rotação [3]

$$E_n(x) = (n + x) \bmod 26$$

$$D_n(x) = (n - x) \bmod 26$$

Cifra de rotação [4]



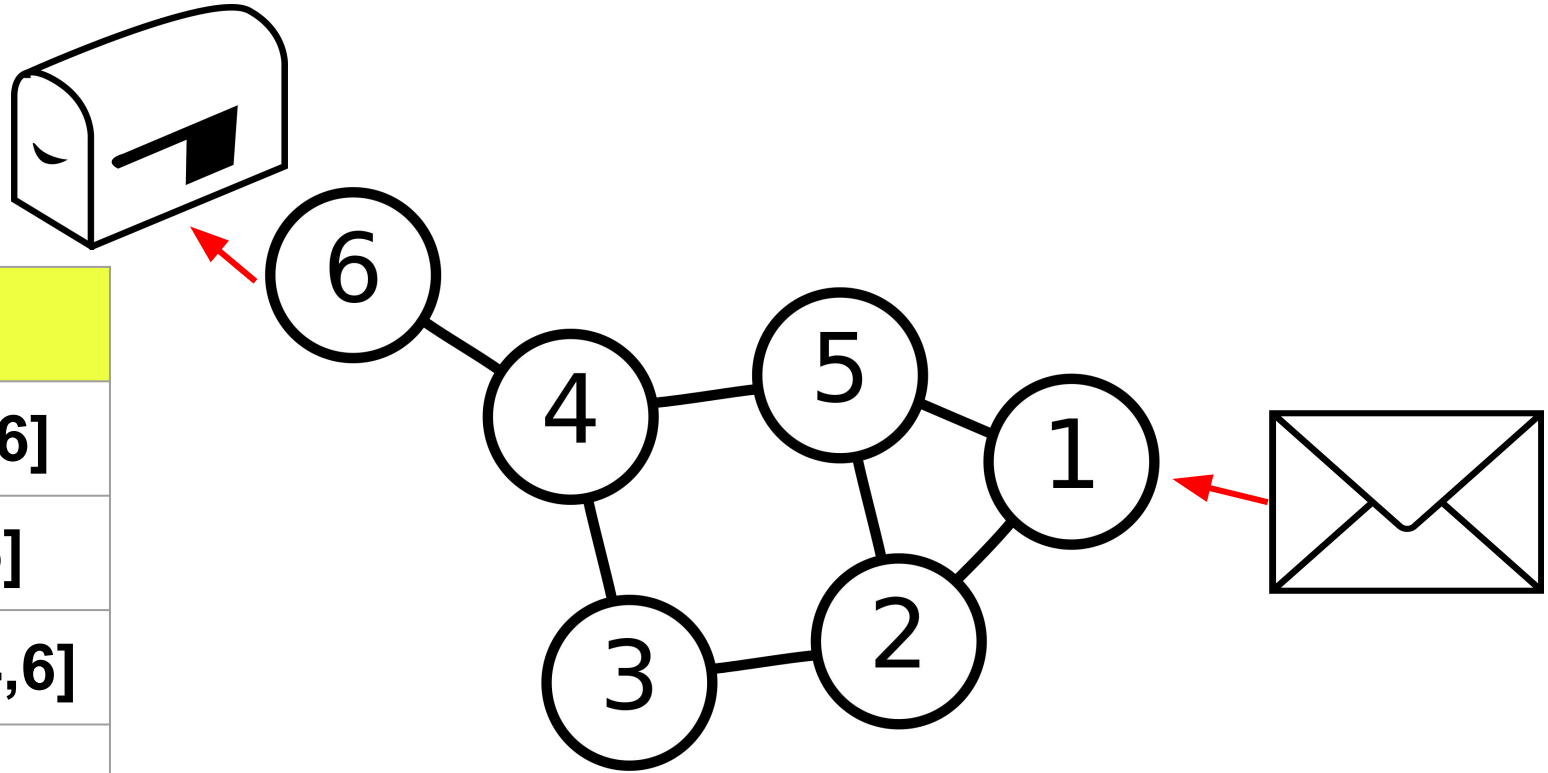
Cifra de rotação [5]

```
1    from string import ascii_uppercase as alphabet
2
3    func = lambda l: alphabet[(alphabet.find(l.upper()) + 13) % 26]
```

Sistemas distribuídos

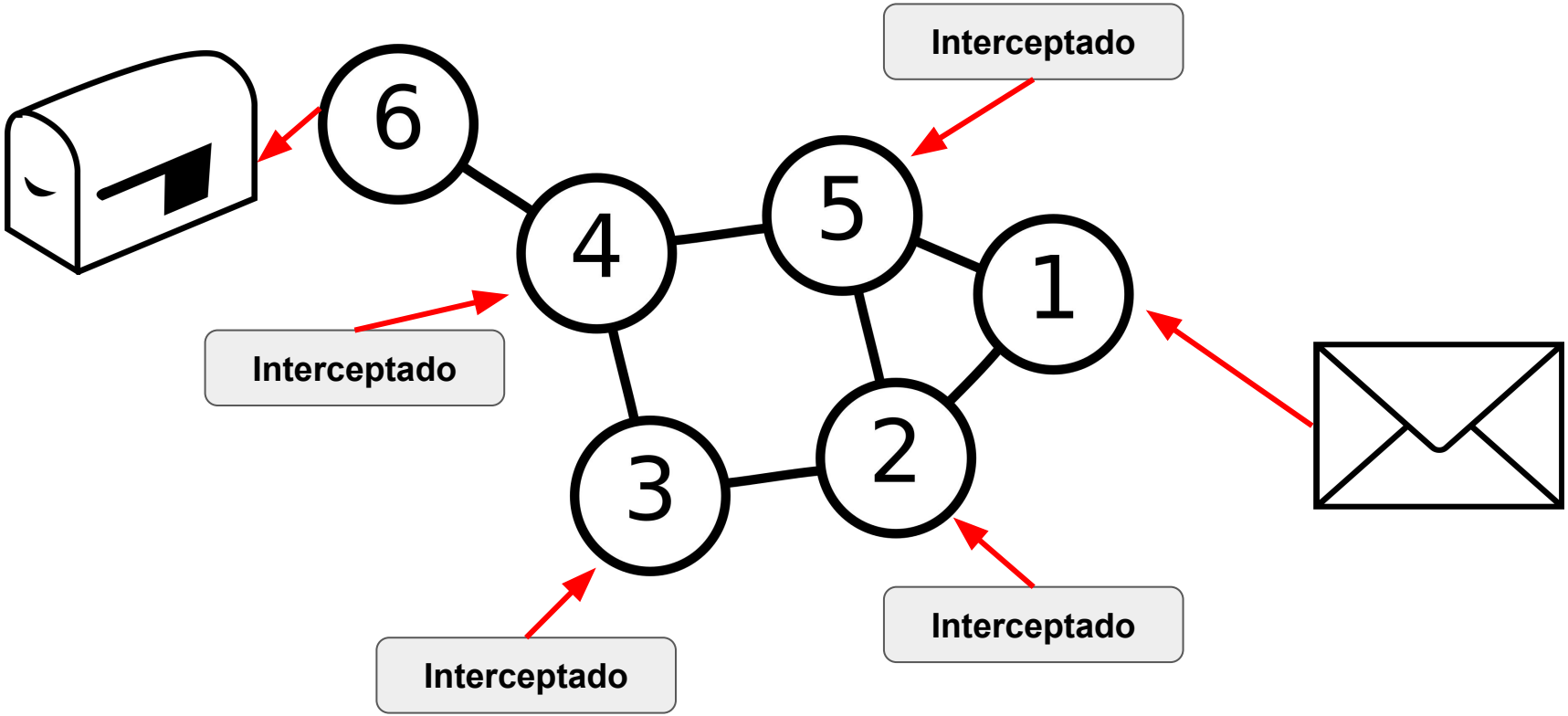
A parte que nos interessa

Sistemas distribuídos [0]



Rotas
[1,2,5,4,6]
[1,5,4,6]
[1,5,2,3,4,6]
...

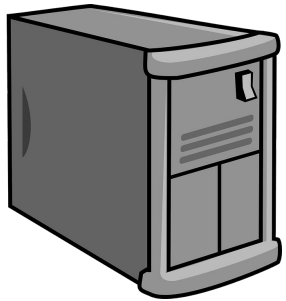
Sistemas distribuídos [0]



Cifras assimétricas

Criptografia na internet

Criptografia de chave pública [0]



Privada

Publica

Servidor de chaves

Publica

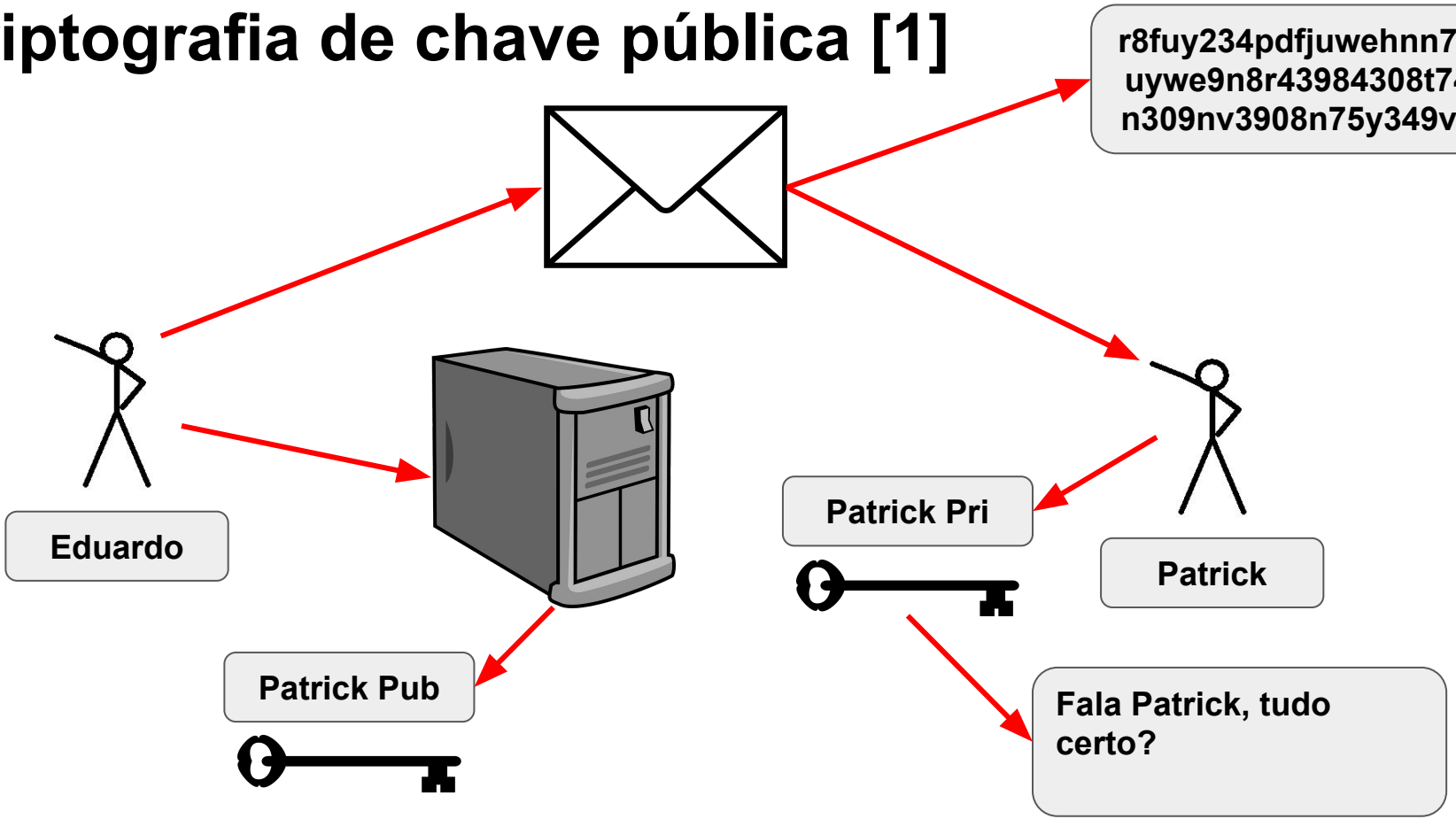
Privada

Patrick

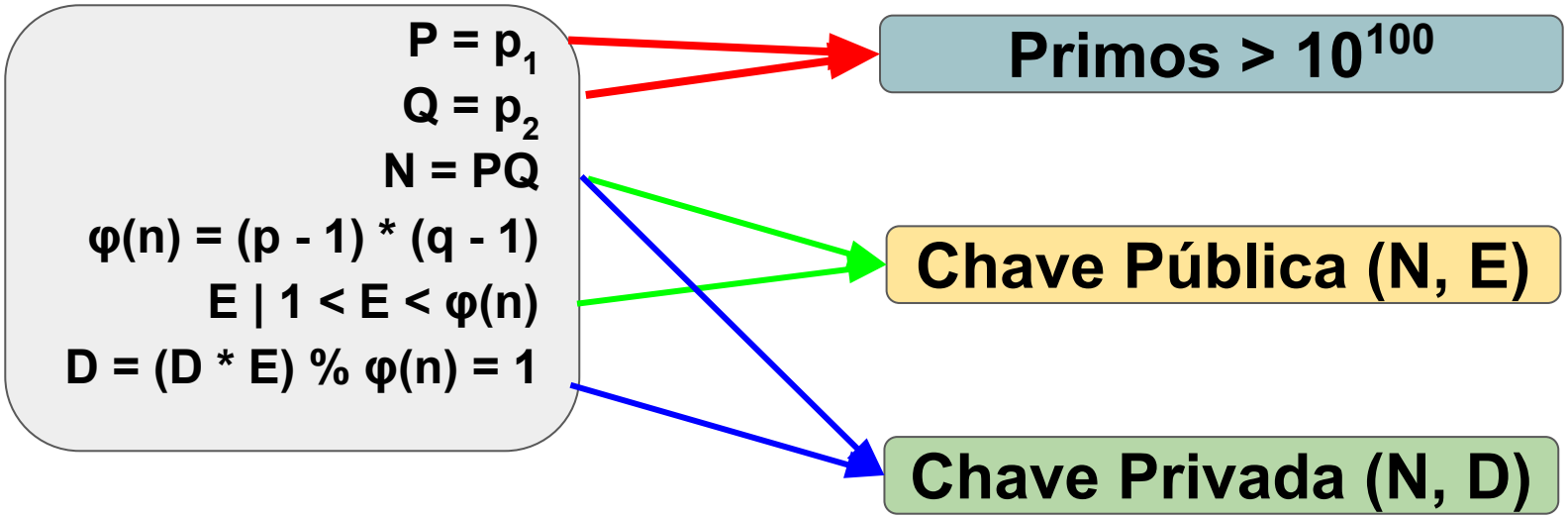
Bob Sponja

User	Chave
Patrick	73yhhb87
Bob Sponja	sjia87y3

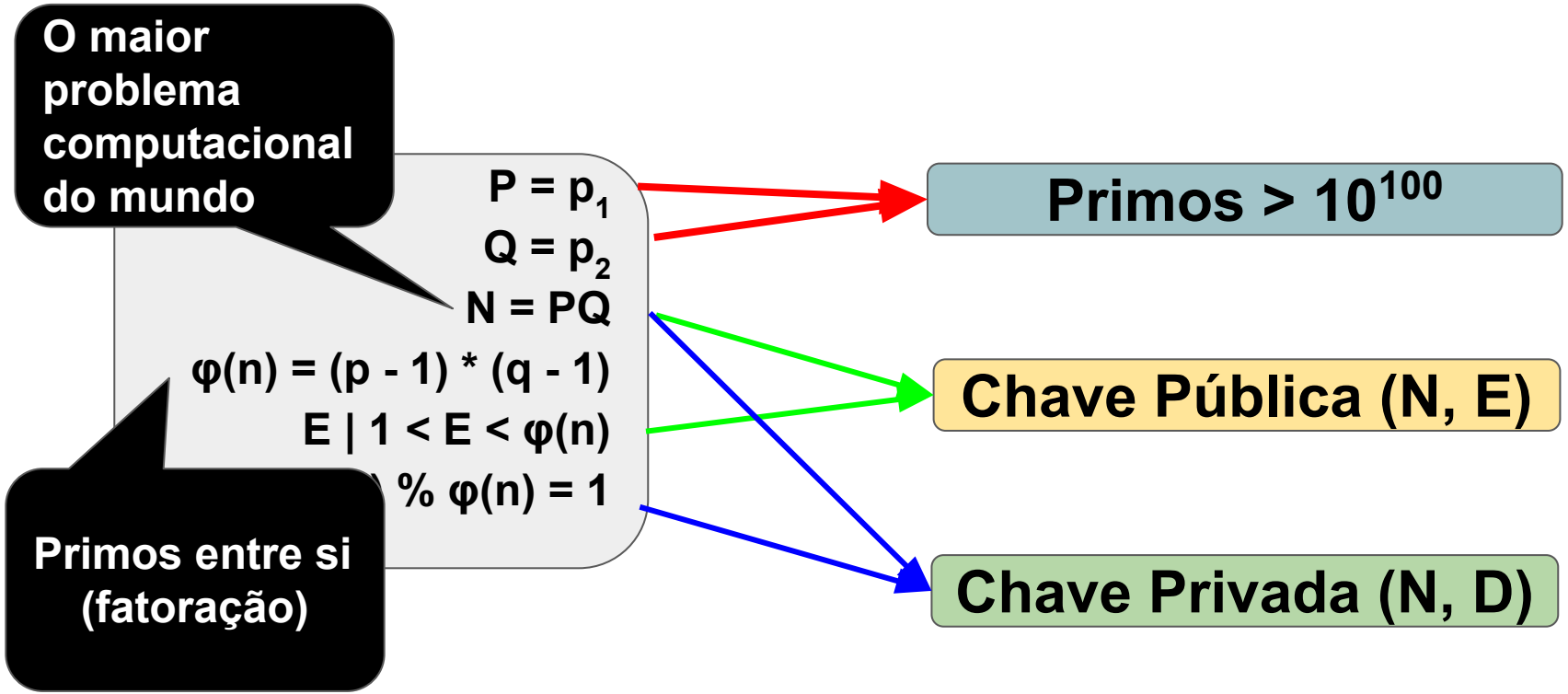
Criptografia de chave pública [1]



Criptografia de chave pública [2] - RSA



Criptografia de chave pública [3] - RSA



Criptografia de chave pública [4] - RSA

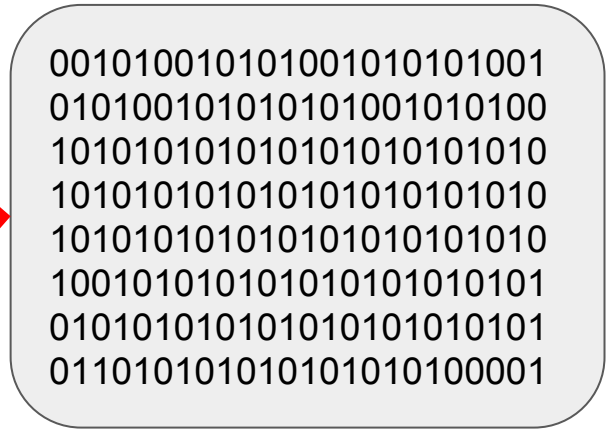
$$c = m^e \pmod{N}$$

$$d = c^e \pmod{N}$$

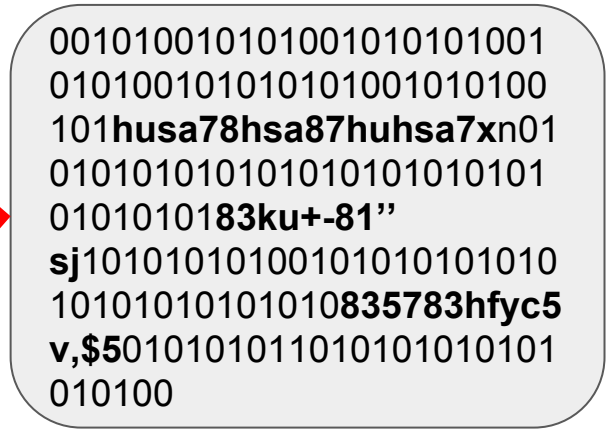
Cifras simétricas

Criptografando arquivos ou dispositivos

Cifra simétrica [0]

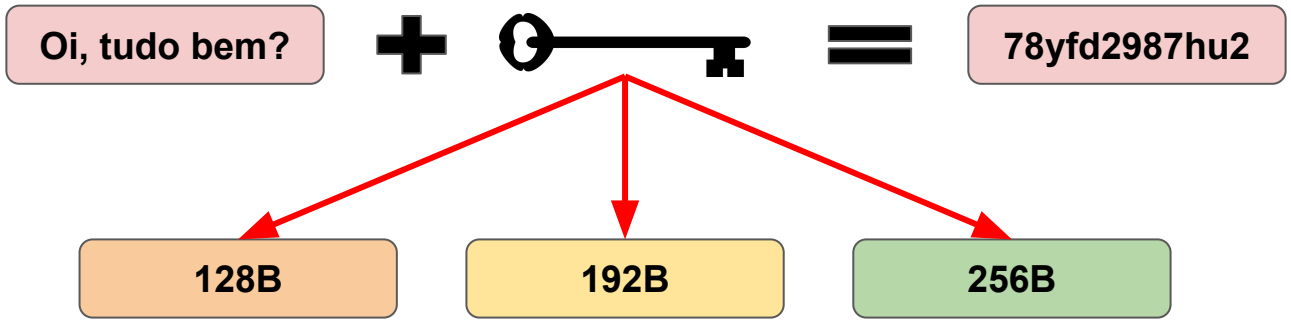


Cifra simétrica [1]

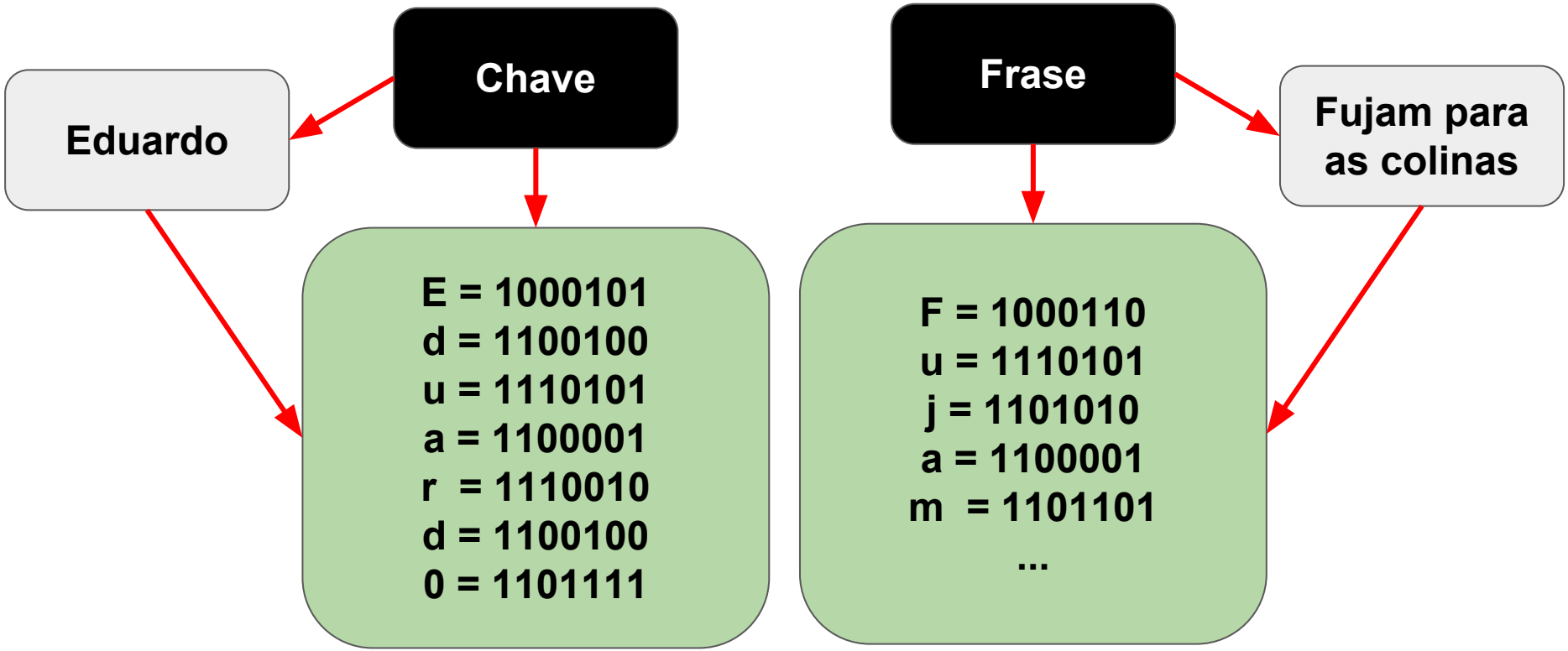


Algorítimos

- AES - O padrão usado hoje em dia
- 3DES - Caindo em desuso
- Twofish - O mais poderoso



Um algorítimo genérico [0]



Um algorítimo genérico [1]

E = 1000101

F = 1000110

Criptografado
E+F = 0000011

1000101
1000110

0000011

Um algorítimo genérico [2]

d = 1100100

u = 1110101

Criptografado
E+F = 0000011
d+u = 1100100

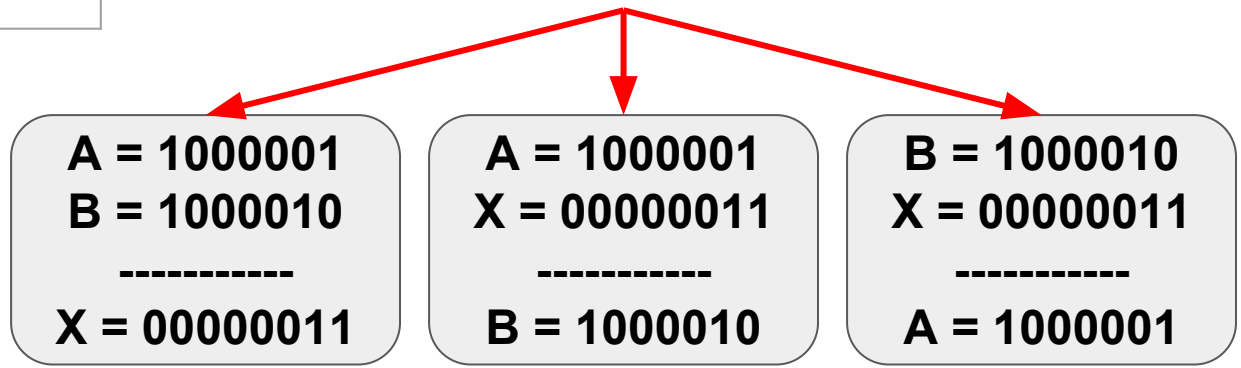
1100100
1110101

0010001

Um algorítimo genérico [3]

Char	Ascii	bin
A	65	1000001
B	66	1000010
X	3	0000011

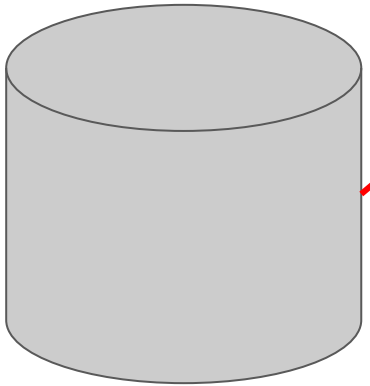
A xor B = X = 00000011
X xor A = B = 1000010
X xor B = A = 1000001



Hash

A parte mais importante de um banco de dados

Diagrama de classe



Cliente
Nome
RG
CPF
Login
Senha

Registro
Patrick Estrela
99.999.999-x
123.456.789-11
P_atrick
lulamolusco

Problemas

- **Qualquer administrador do banco pode saber todas as senhas**
- **Qualquer ataque de força bruta pode acessar nosso sistema**
- **Caso o sistema seja invadido todos os seus usuários estarão comprometidos**

Senha x Hash

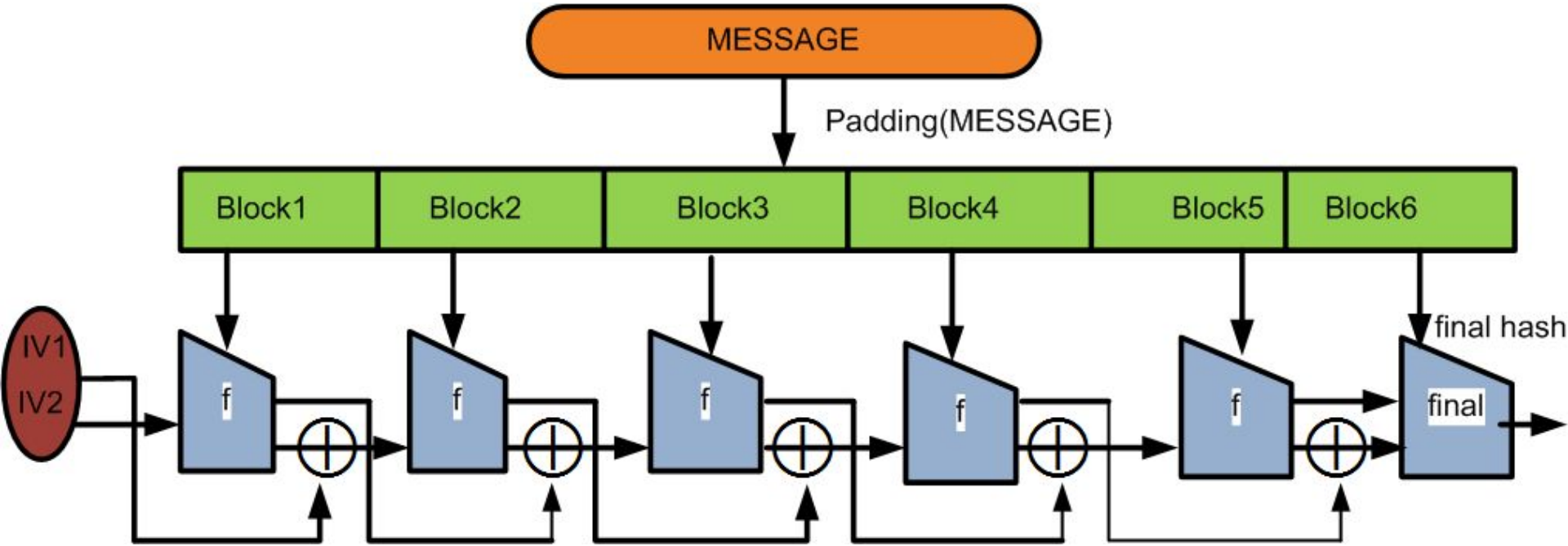
Eduardo(MD5):
ba3615ba56f5b0b7c6a206fba90d8e4a

Eduardo (sha1):
c6793f32da227a30f87d8deeeb8dd70dc0ada615

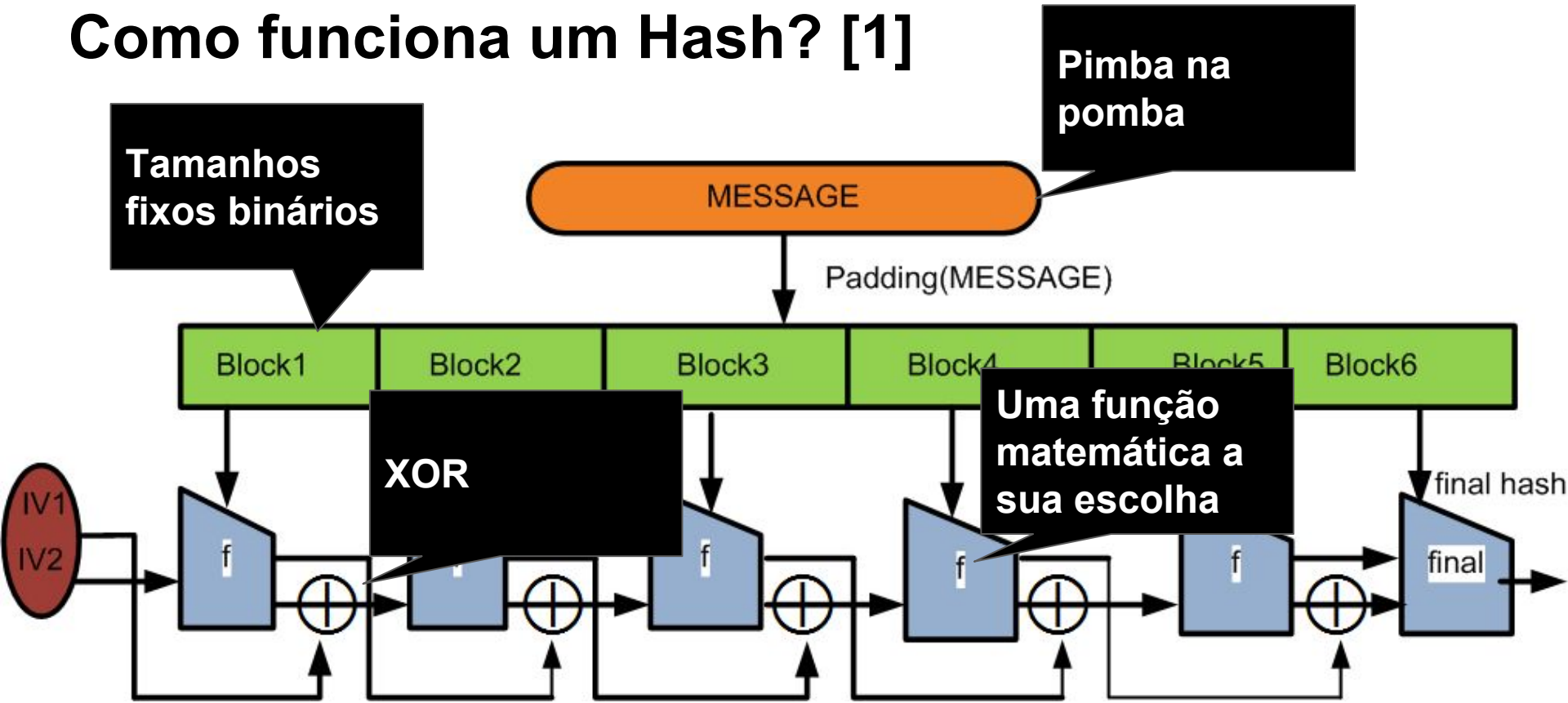
Eduardo(sha256):
bdf58324e184b654bbbe386a3500f09937f1aad5e44edd80d61421c6ffd4aa6c

Eduardo(sha512):
fb409b32edce08f78b1c0bca70b7d524e75e951b2ece4aaa6ac61c359efb53e10
0d2a2e2c7d03566f9084f0e16f2228d90095acaae79f3eae79766833e7a69df

Como funciona um Hash? [0]



Como funciona um Hash? [1]



XOXO

Duvidas?

mendesxeduardo@gmail.com