Plaintext : Isto é **u**m teste

Chave : asjhiu**t**iuysadlksjfl

Ciphertext : fiuoid**g**lkjewrpi

**Cifra simétrica**

Key: 011011011011 v v 011011011011

PT: 01011001110 🡪 0100110111 🡪 01011001110

XOR XOR

A | B = C | B = A

0 | 0 = 0 | 0 = 0

0 | 1 = 1 | 1 = 0

1 | 0 = 1 | 0 = 1

1 | 1 = 0 | 1 = 1

A = Plaintext

B = Key

C = Ciphertext

XOR 🡪 mod 2

**Cifras assimétricas**

Bob:

- Chave privada (PrB)

- Chave publica (PuB)

Alice:

- PrA

- PuA

Bob ---> Alice

Enc(Plaintext, PrB, PuA) ----> Ciphertext ----> Desenc(Ciphertext, PrA, PubB)