

#4 Symmetric Cryptography

SEGURANÇA NAS ORGANIZAÇÕES E INFORMÁTICA

deti universidade de aveiro
departamento de eletrónica,
telecomunicações e informática

2024/2025

About Cryptography

What is it (in simple terms) ?

Securing communication and information so that it is unintelligible to unwanted entities

Information is subjected to several (reversible) operations that should only be known to those who know the keys or process.

About Cryptography

The two flavors

Symmetric

One key for everything

All participants know the same information.

Asymmetric

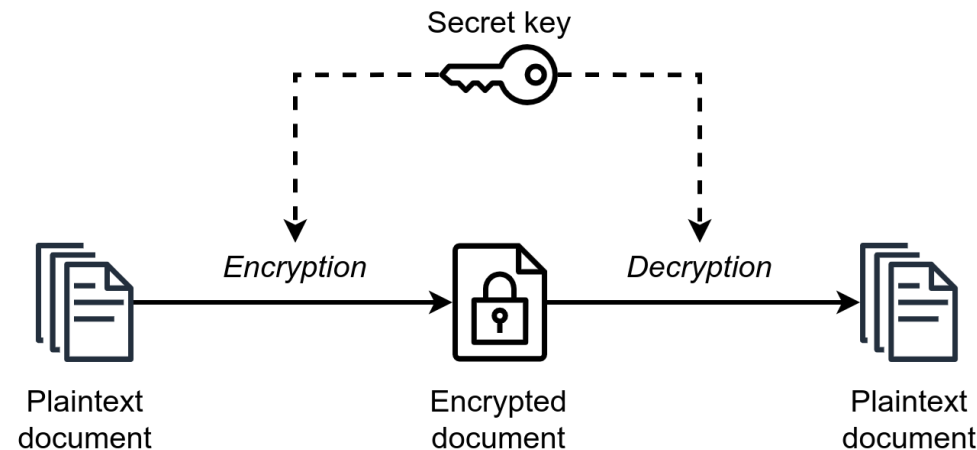
A key pair for diferente operations

Different participants have different material

About Symmetric Encryption

What is it (in simple terms) ?

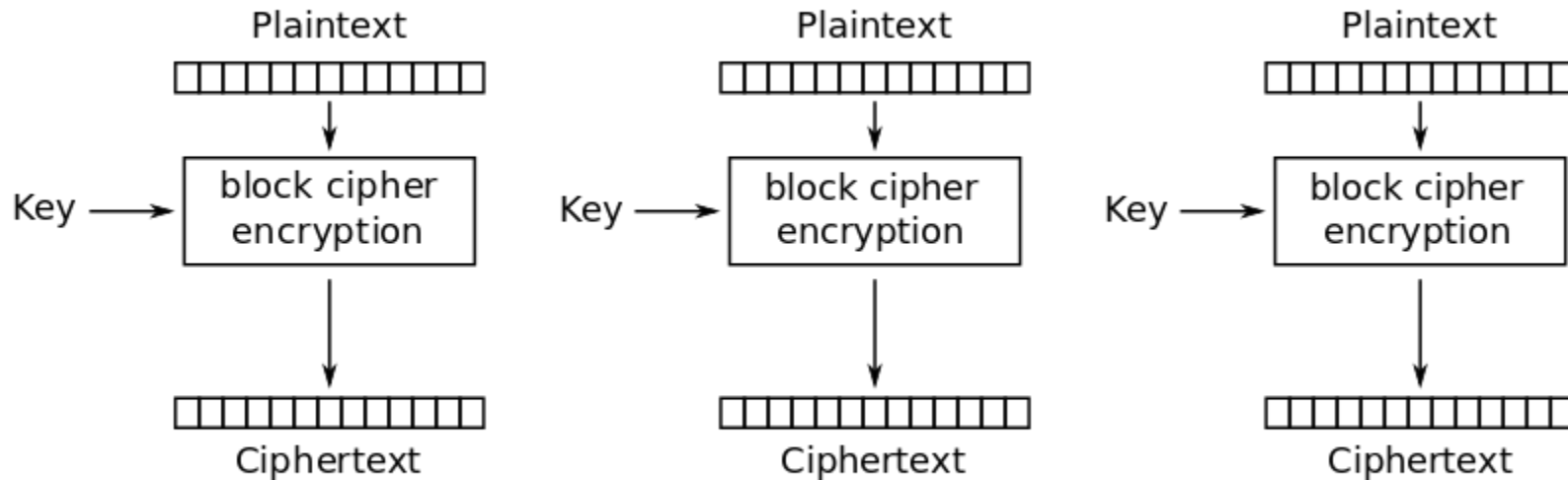
It is the process of using the **same shared secret** to cipher and decipher data



https://en.wikipedia.org/wiki/Symmetric-key_algorithm

Symmetric Encryption Modes

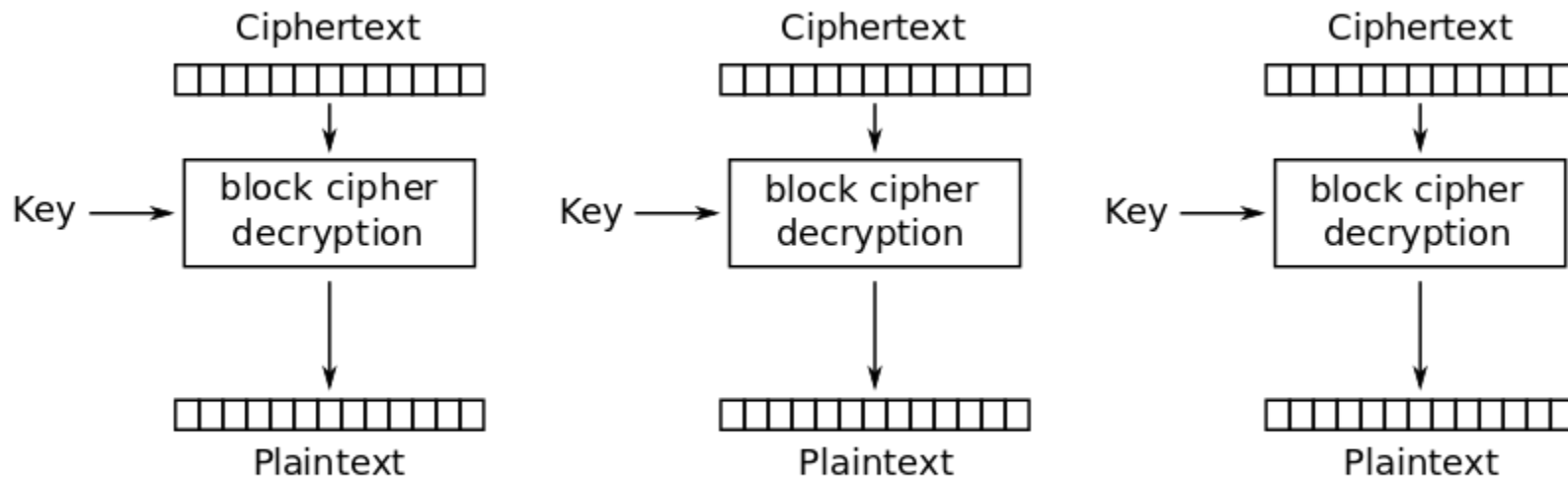
Block Cipher Modes of Operation - ECB - Encryption



Electronic Codebook (ECB) mode encryption

Symmetric Encryption Modes

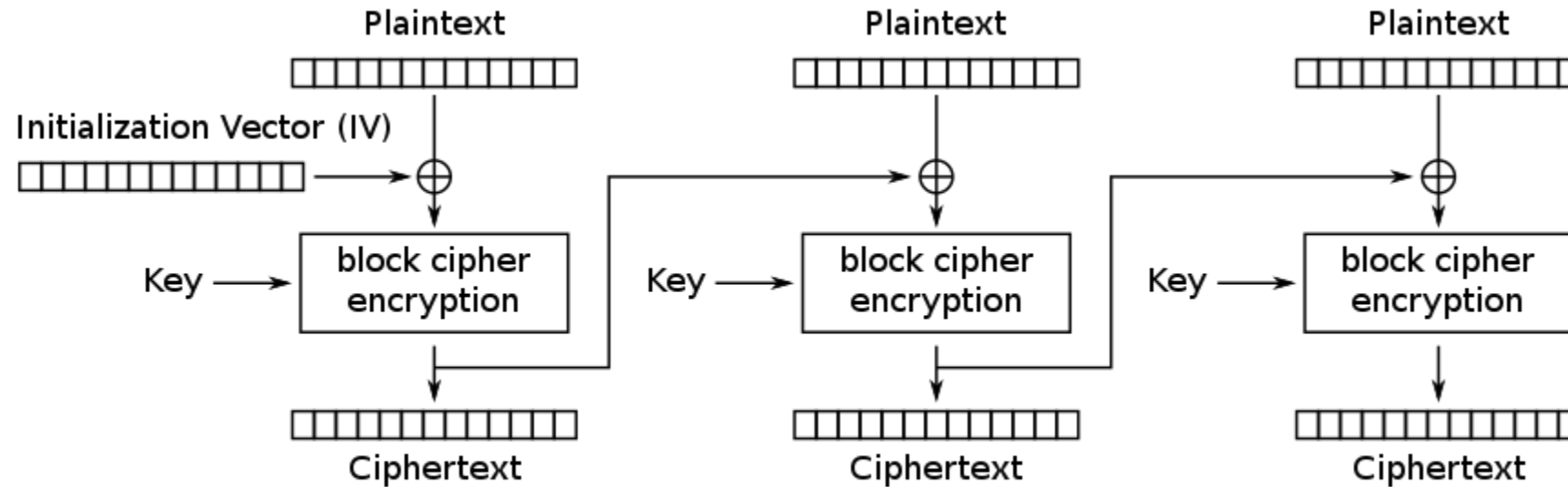
Block Cipher Modes of Operation - ECB - Decryption



Electronic Codebook (ECB) mode decryption

Symmetric Encryption Modes

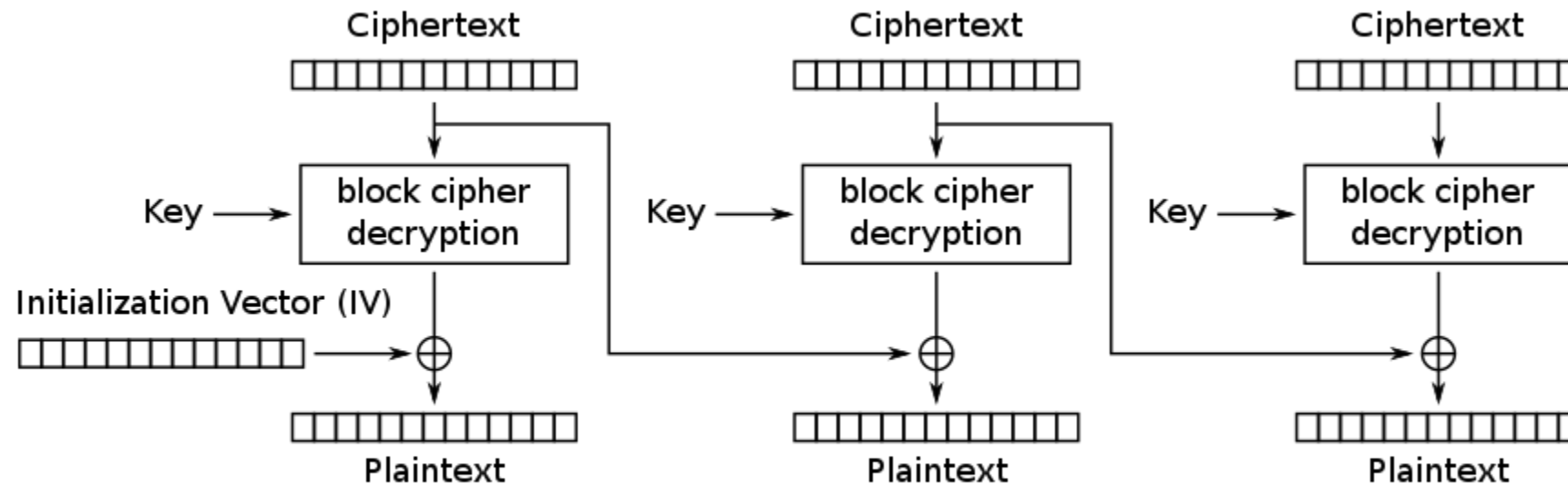
Block Cipher Modes of Operation - CBC - Encryption



Cipher Block Chaining (CBC) mode encryption

Symmetric Encryption Modes

Block Cipher Modes of Operation - CBC - Decryption



Cipher Block Chaining (CBC) mode decryption

Padding

Why it is needed?

- Blocks need to have a well-known size to be ciphered
- All blocks must be complete
- AES has a 128 bit blocks

But what if the message is not a multiple of 128 bits?

Padding

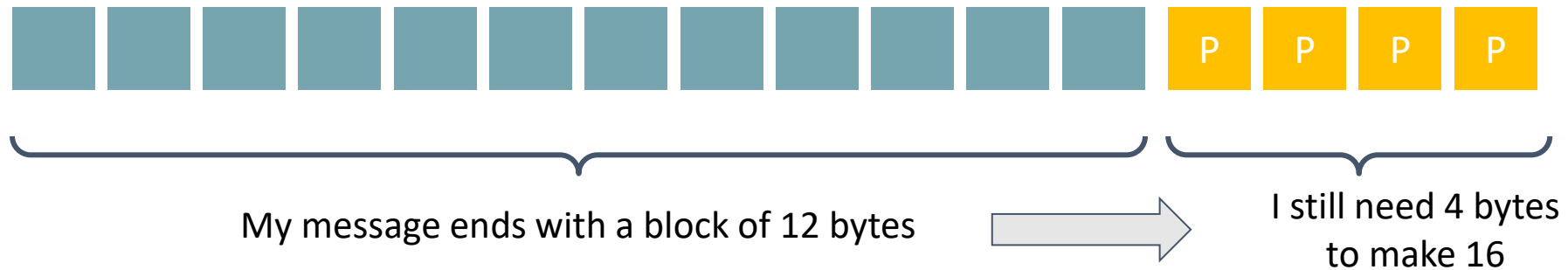
Simple Example



My message ends with a block of 12 bytes

Padding

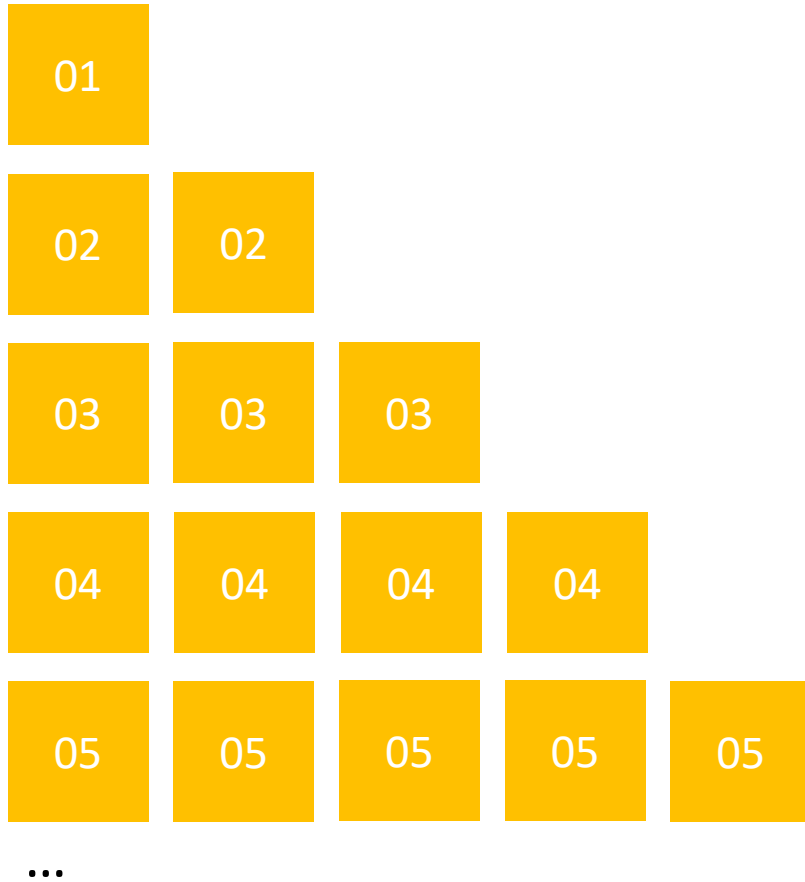
Simple Example



But keep in mind, padding needs to be identifiable!

Padding

PKCS-7



The padding is n bytes
whose value is n