#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.

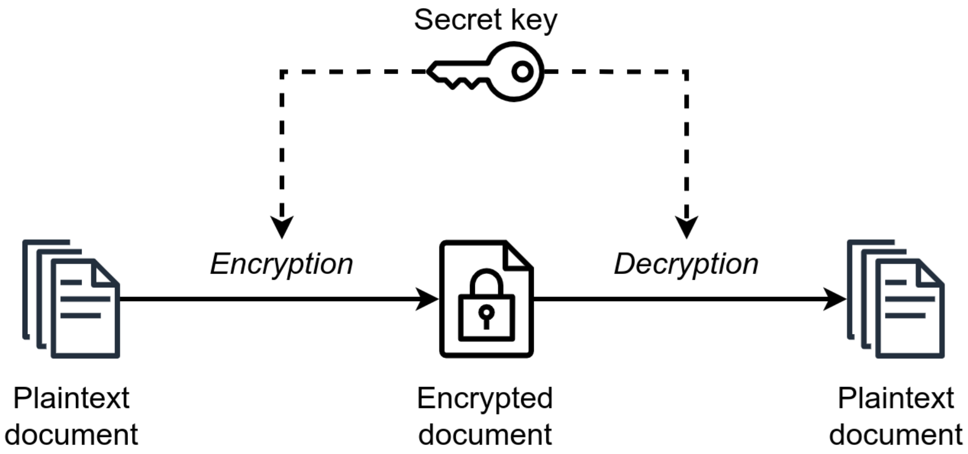
Asymmetric
A key pair for diferente operations

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



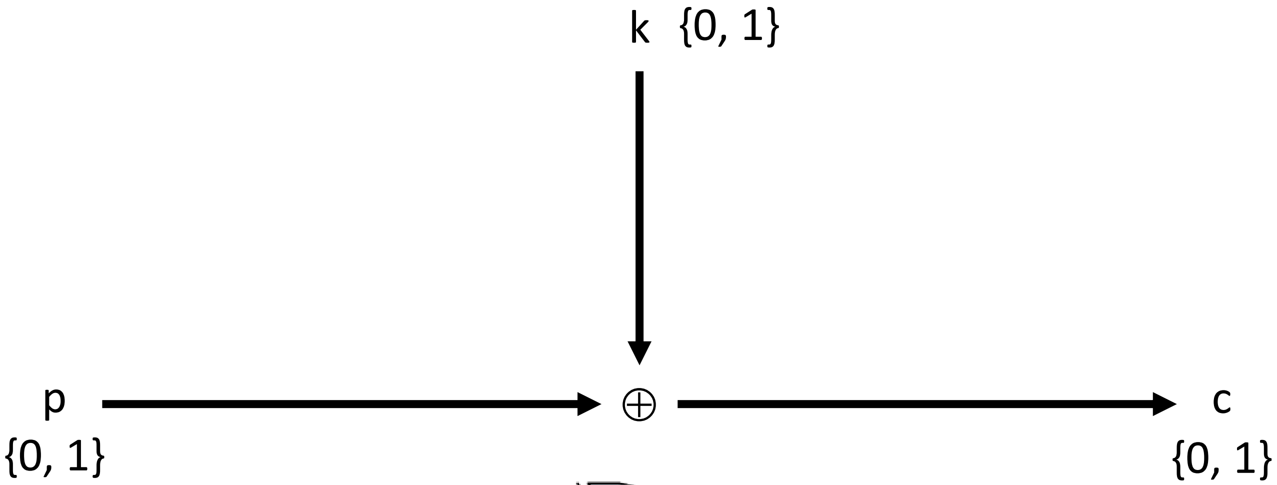
https://en.wikipedia.org/wiki/Symmetric-key_algorithm

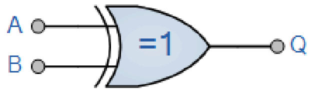
Symmetric Cryptography

i.e., the same key is used to encrypt and decrypt

One Time Pad

(Vernam, according to the US Patents Office -- disputed)





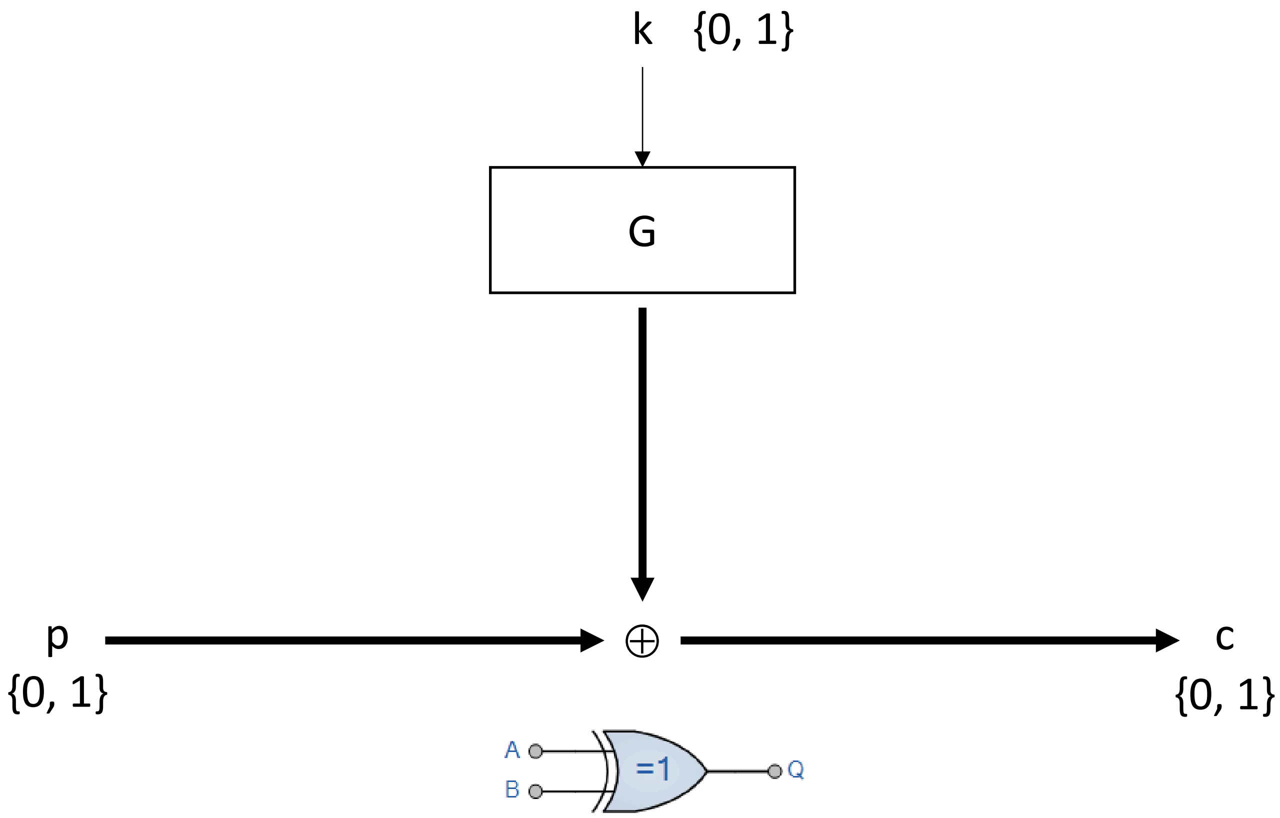
k	p	c
0	0	0
0	1	1
1	0	1
1	1	0

If k is truly random

$P_c(0) = 1/2$

$P_c(1) = 1/2$

Symmetric Cryptography



G	p	c
0	0	0
0	1	1
1	0	1
1	1	0

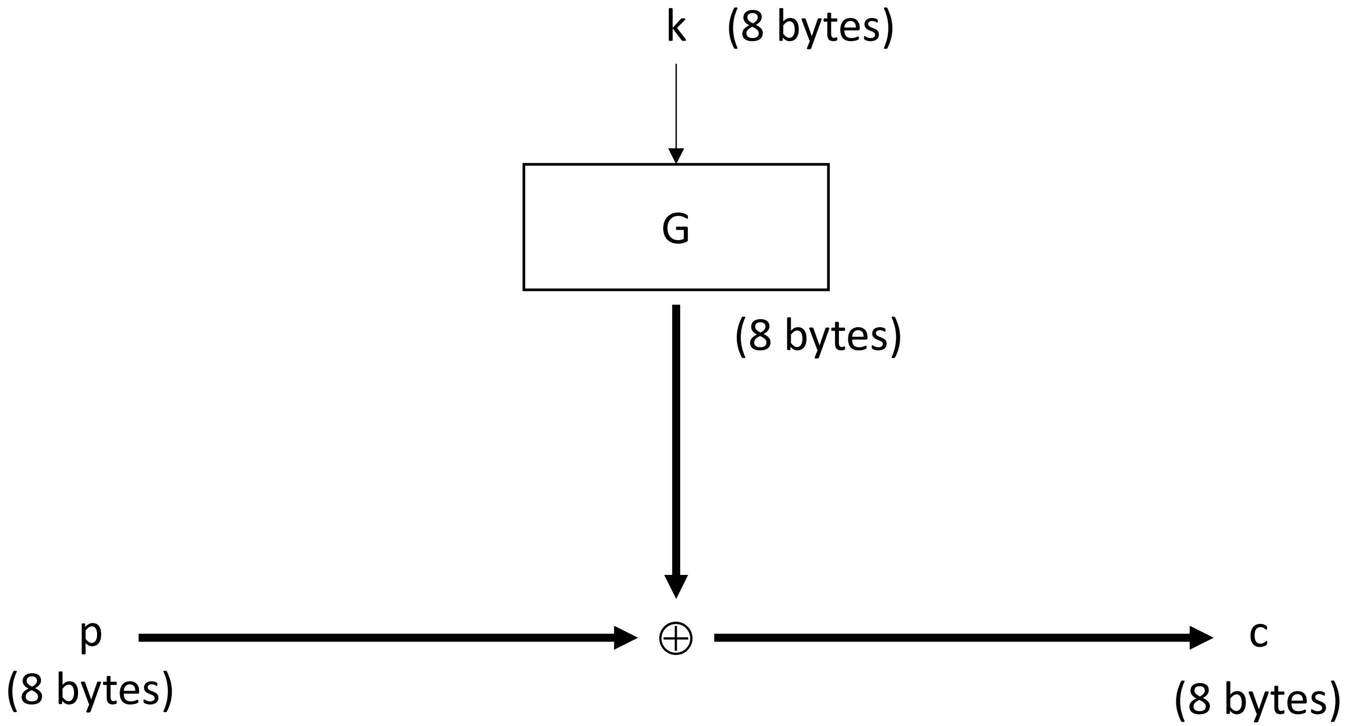
If G is not truly random:

$P_c(0) = ½ + \varepsilon$

$P_c(1) = ½ + \varepsilon$

Computationally Secure
if $\varepsilon < E$

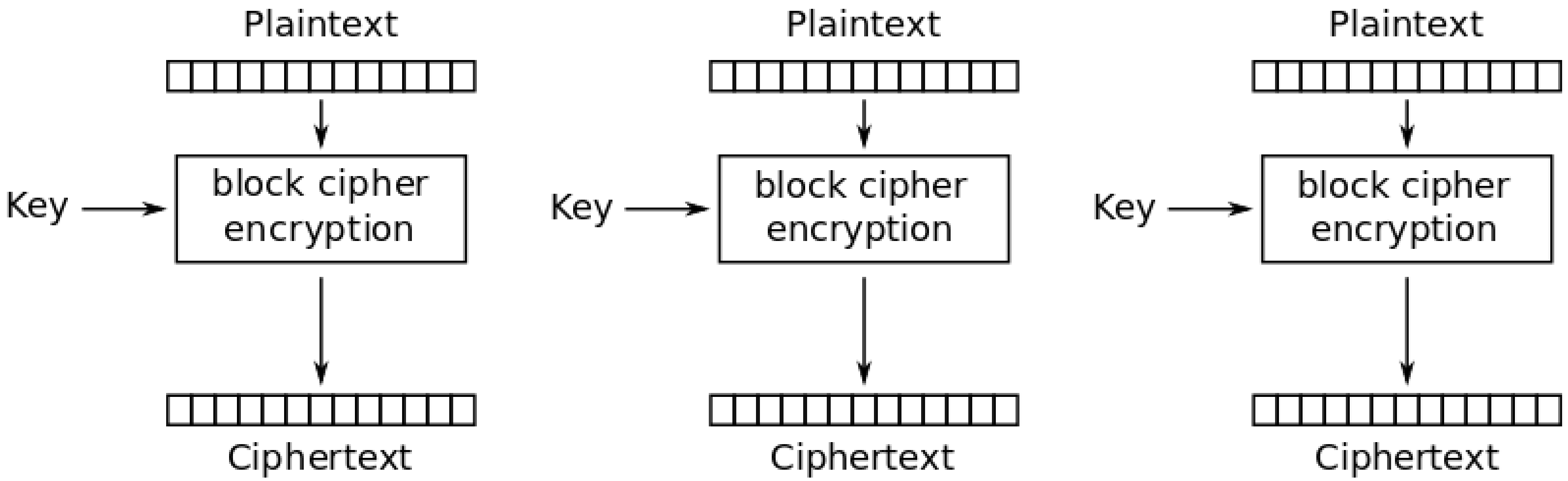
Symmetric Cryptography



Block ciphers help keep $\varepsilon < E$

Symmetric Encryption Modes

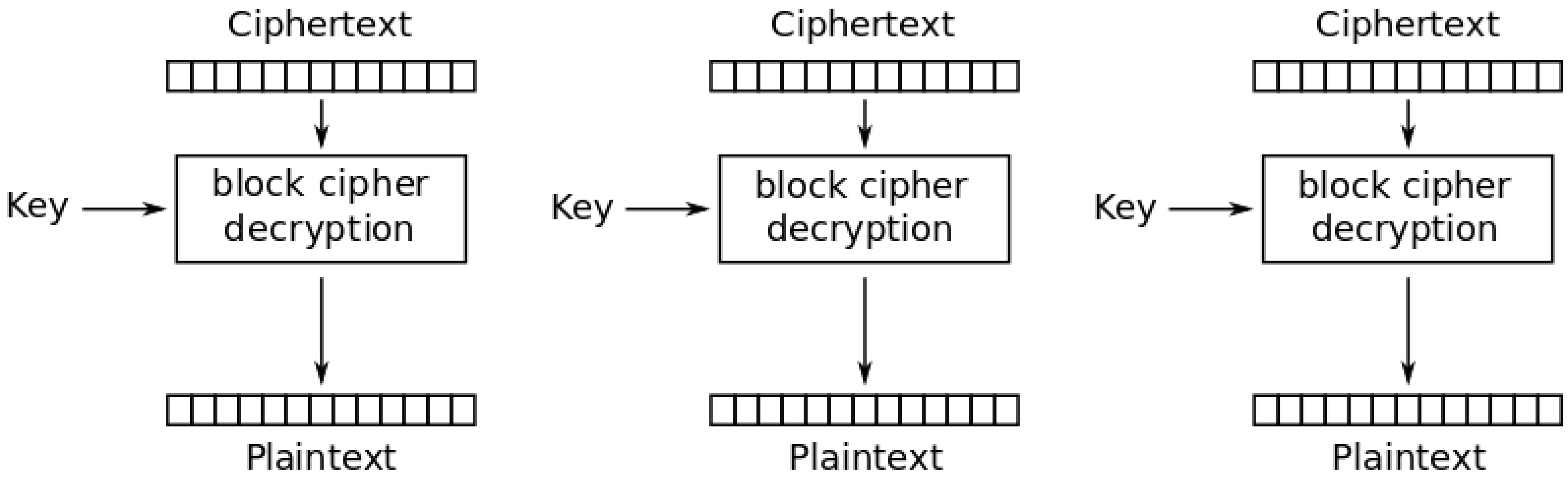
Block Cipher Modes of Operation - ECB - Encryption



Electronic Codebook (ECB) mode encryption

Symmetric Encryption Modes

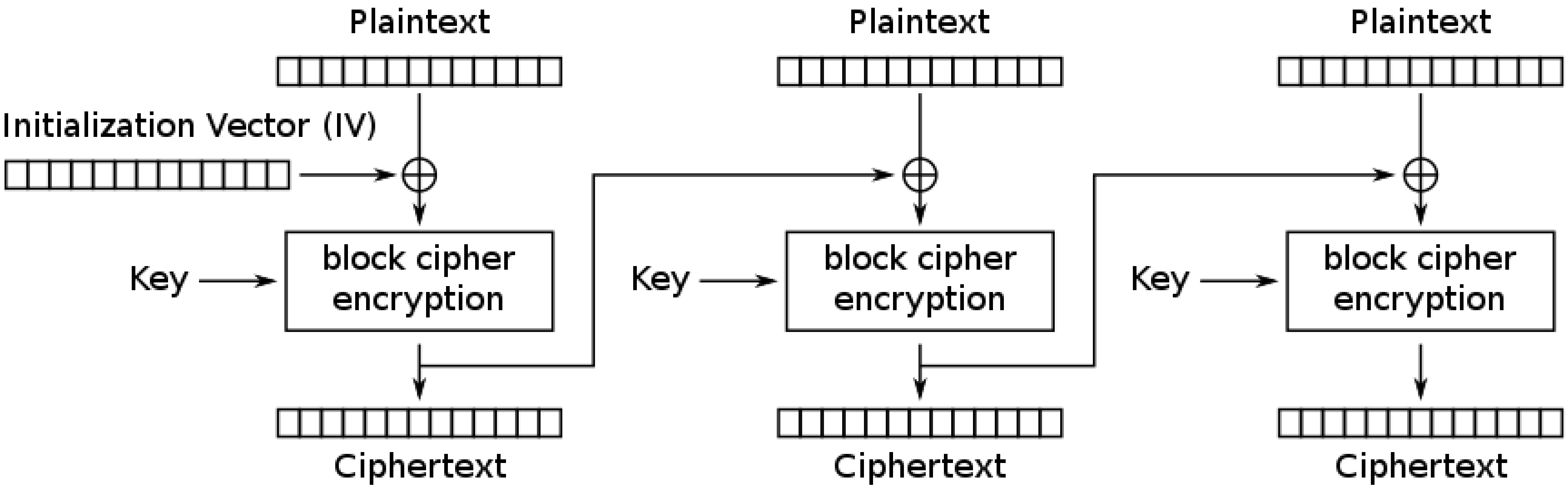
Block Cipher Modes of Operation - ECB - Decryption



Electronic Codebook (ECB) mode decryption

Symmetric Encryption Modes

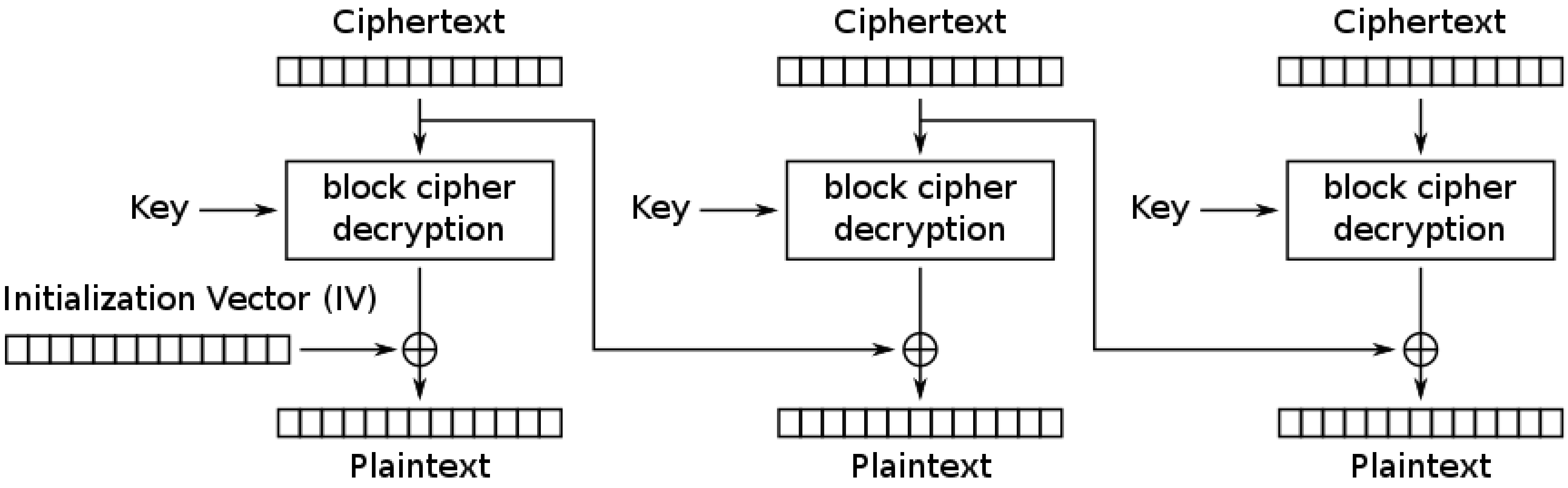
Block Cipher Modes of Operation - CBC - Encryption



Cipher Block Chaining (CBC) mode encryption

Symmetric Encryption Modes

Block Cipher Modes of Operation - CBC - Decryption



Cipher Block Chaining (CBC) mode decryption

Padding

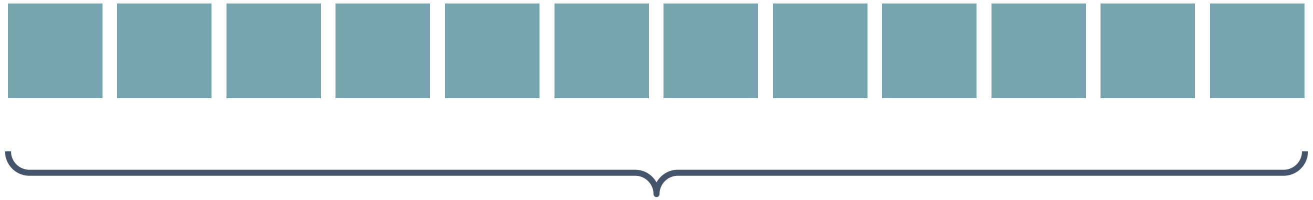
Why it is needed?

- 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

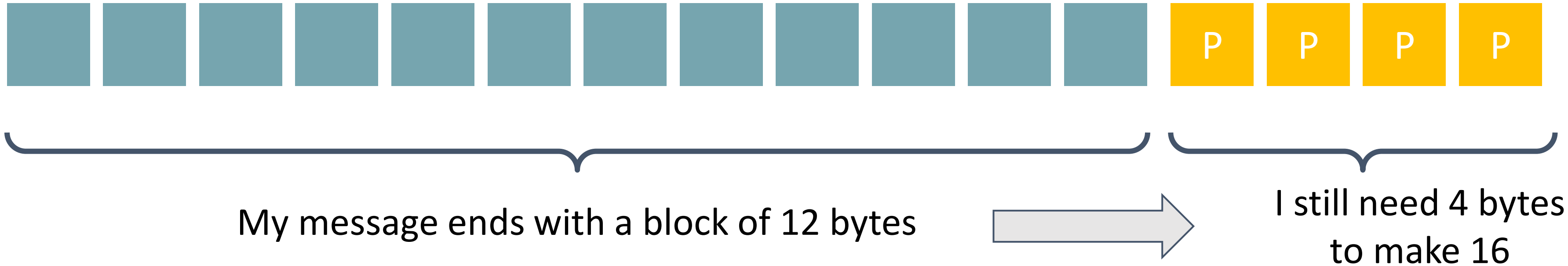
Simple Example



My message ends with a block of 12 bytes

Padding

Simple Example



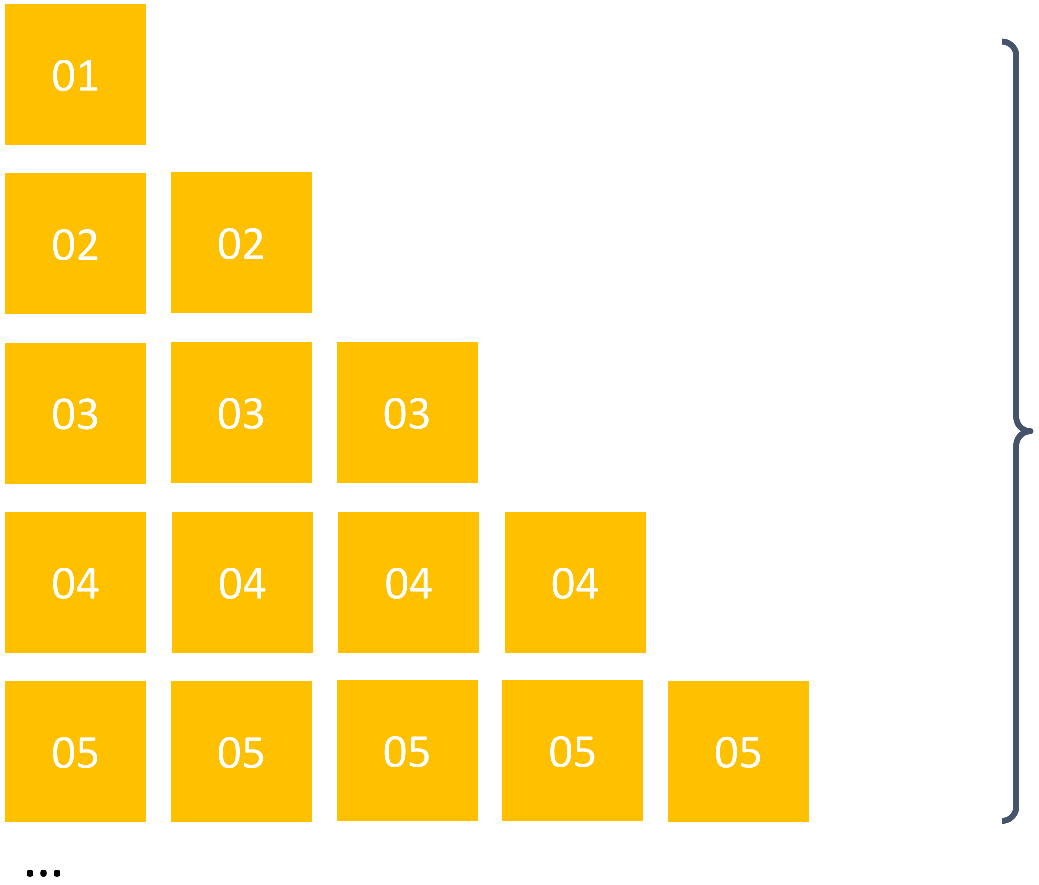
My message ends with a block of 12 bytes

I still need 4 bytes
to make 16

But keep in mind, padding needs to be identifiable!

Padding

PKCS-7



01

02 02

03 03 03

04 04 04 04

05 05 05 05 05

…

The padding is *n* bytes whose value is *n*

Practical Guide

Overview

✓Three fundamental topics:

- Symmetric encryption
- Symmetric Padding
- Key Derivation Functions.

✓Use a python cryptography library:

- cryptography.io module
- “hazardous materials” documentation

Cryptographic operations

Encrypting and decrypting

```
import os
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes


cipher = Cipher(algorithms.AES(key), modes.CBC(iv))

pt  = b"a secret message"
encryptor = cipher.encryptor()
ct = encryptor.update(pt) + encryptor.finalize()

decryptor = cipher.decryptor()
dt = decryptor.update(ct) + decryptor.finalize()
```

Cryptographic operations

Padding

```
from cryptography.hazmat.primitives import padding


padder = padding.PKCS7(128).padder()
padded_data = padder.update(b"text")
padded_data += padder.finalize()


unpadder = padding.PKCS7(128).unpadder()
data     = unpadder.update(padded_data)
original = data + unpadder.finalize()
```

Cryptographic operations

Password-based Key derivation

```python
import os
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.kdf.pbkdf2 import PBKDF2HMAC



salt = os.urandom(16)
kdf = PBKDF2HMAC(
    algorithm=hashes.SHA256(),
    length=32,
    salt=salt,
    iterations=480000,
)
key = kdf.derive(b"my password")
```

Image encryption outputs

ECB

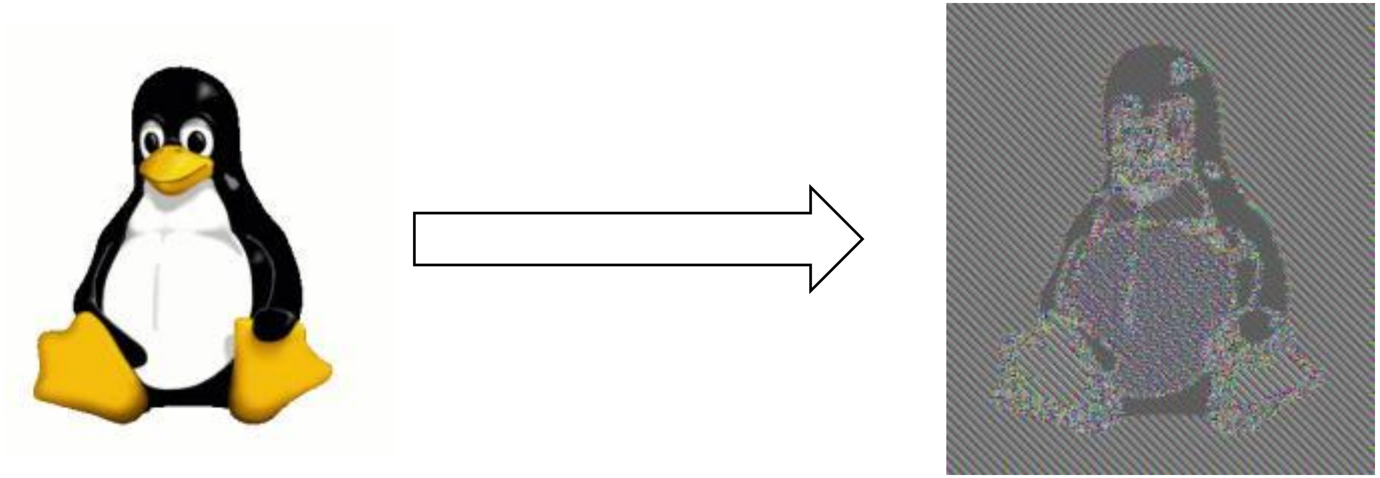


Image encryption outputs

CBC