#5 Asymmetric Cryptography

SEGURANÇA NAS ORGANIZAÇÕES E INFORMÁTICA

deti universidade de aveiro
departamento de eletrónica, telecomunicações e informática

2024/2025

About Cryptography

Recap

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 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

Fast and simple but has drawbacks

- Involved parties need to share the same key
- Needs a secure channel to share keys (can be hard)
- Keys do not to distinguish any involved parties
- Distribution does not scale

About Asymmetric Cryptography

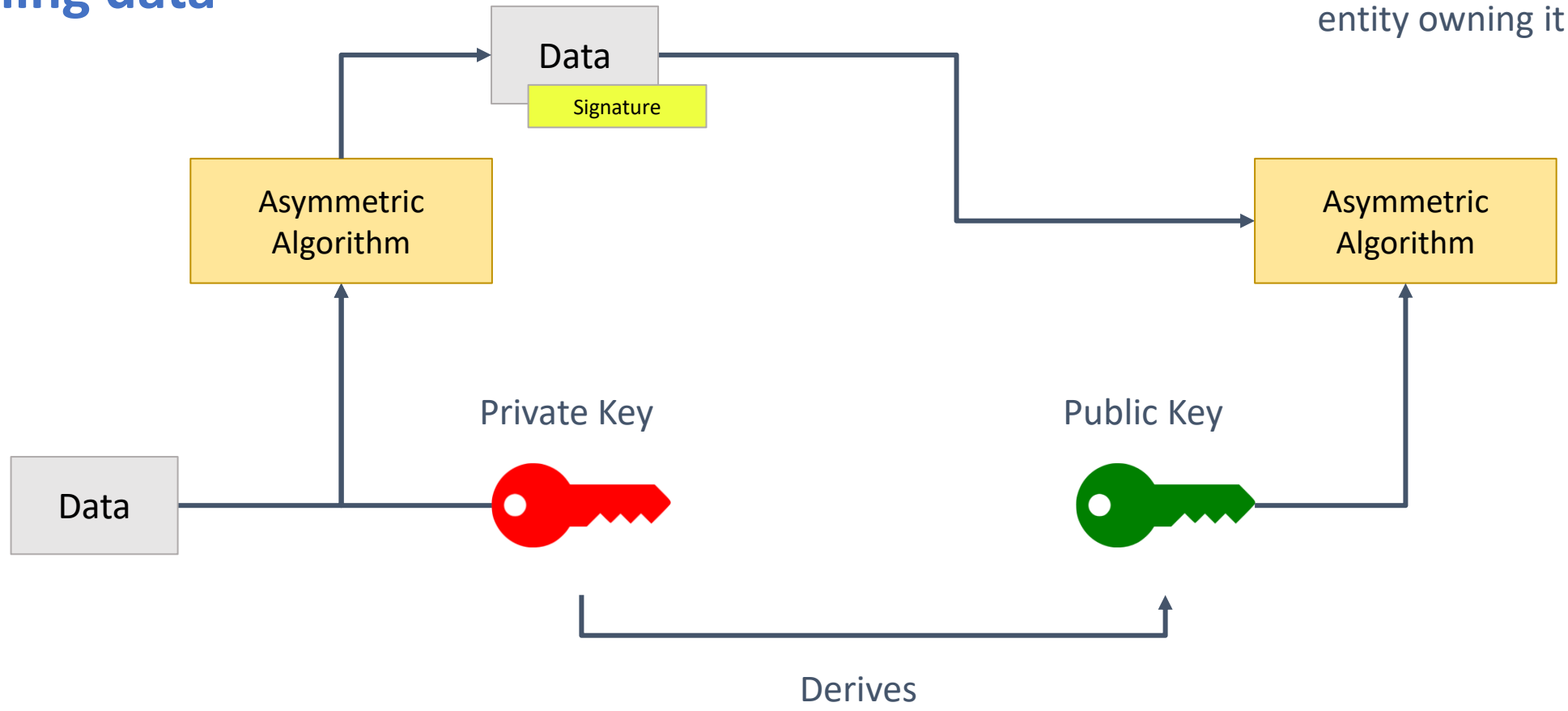
What is it?

It is the process of using a pair of keys to secure and authenticate data

Private Key

Signing data

If the Public Key was derived from the Private key, we can verify the data signature came from the entity owning it!

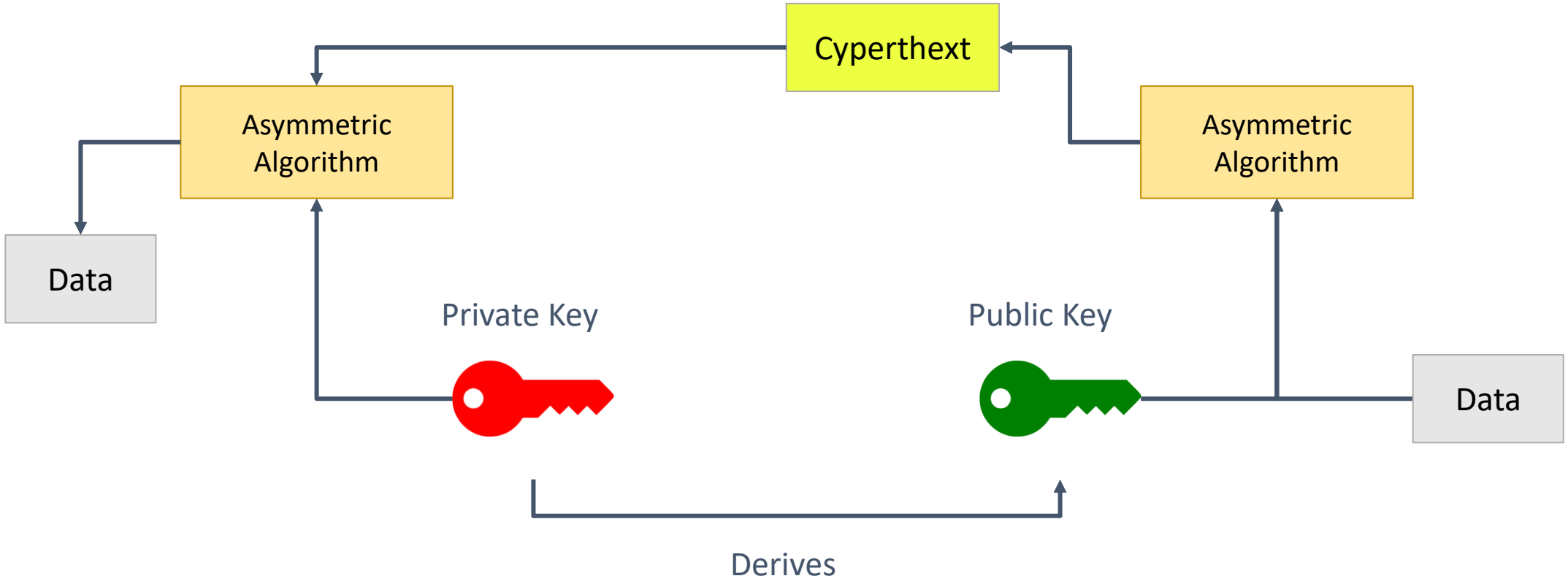


We can use this mechanism to verify authenticity

Public Key

Encrypting data

If the Public Key was derived from the Private key, we can you the private key to decipher the data!



We can use this mechanism to share secret information

About Cryptography

The two flavors

Symmetric

One key for everything

All participants know the same information.

Fast and simple but has drawbacks

- Involved parties need to share the same key
- Needs a secure channel to share keys (can be hard)
- Keys do not to distinguish any involved parties
- Distribution does not scale

Asymmetric

A key pair for diferente operations

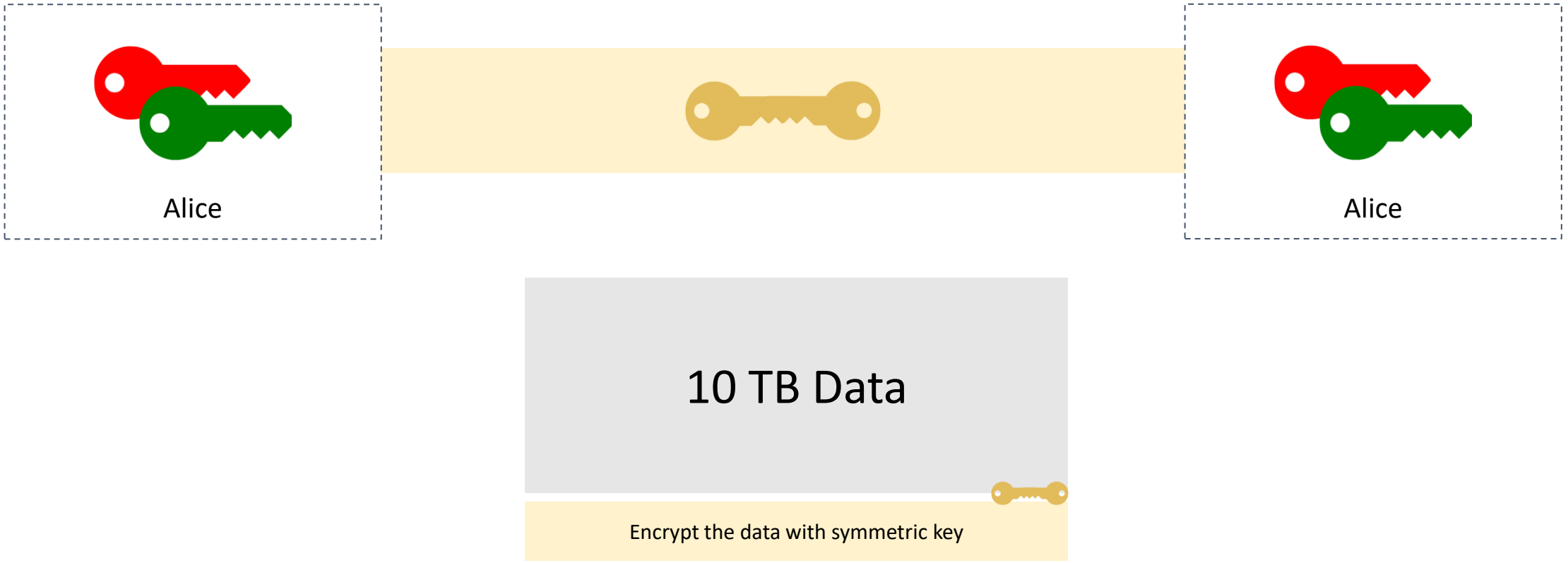
Different participants have different material

Very secure but has drawbacks

- Slow and complex
- Computationally intensive (expensive)

Asymmetric + Symmetric

A simple scenario



Asymmetric cryptography to share the secret key and symmetric to cipher data