# Fundamentos de Segurança Informática

2025/2026

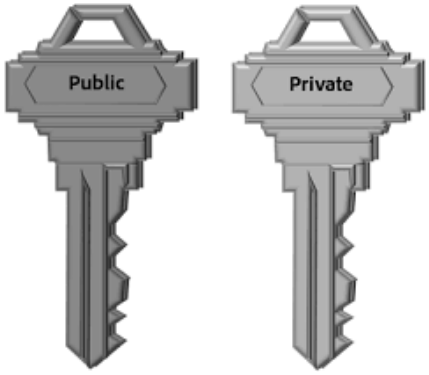
---

# Aulas Práticas #1

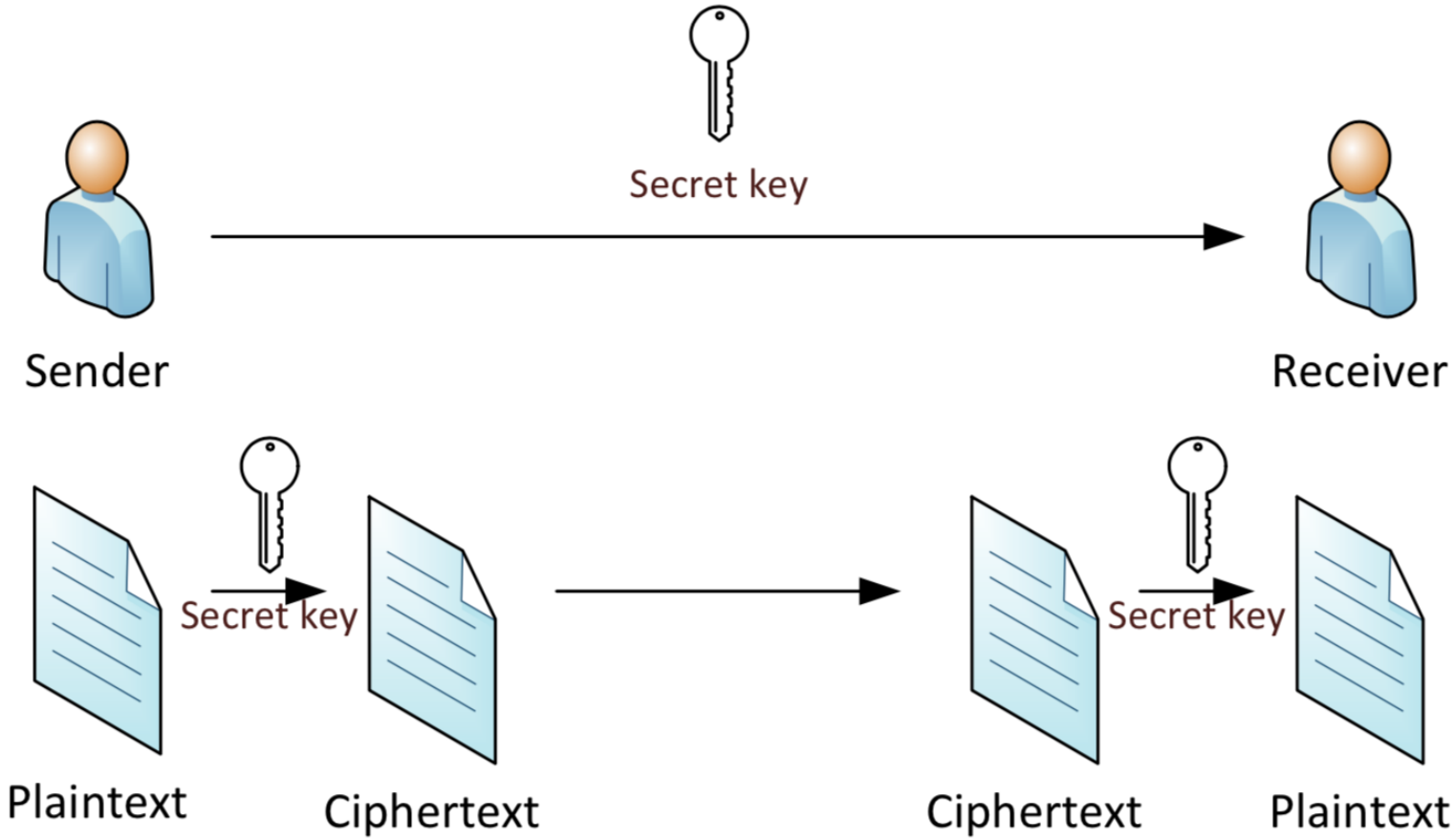
## - PGP (Pretty Good Privacy)

# Sistemas criptográficos

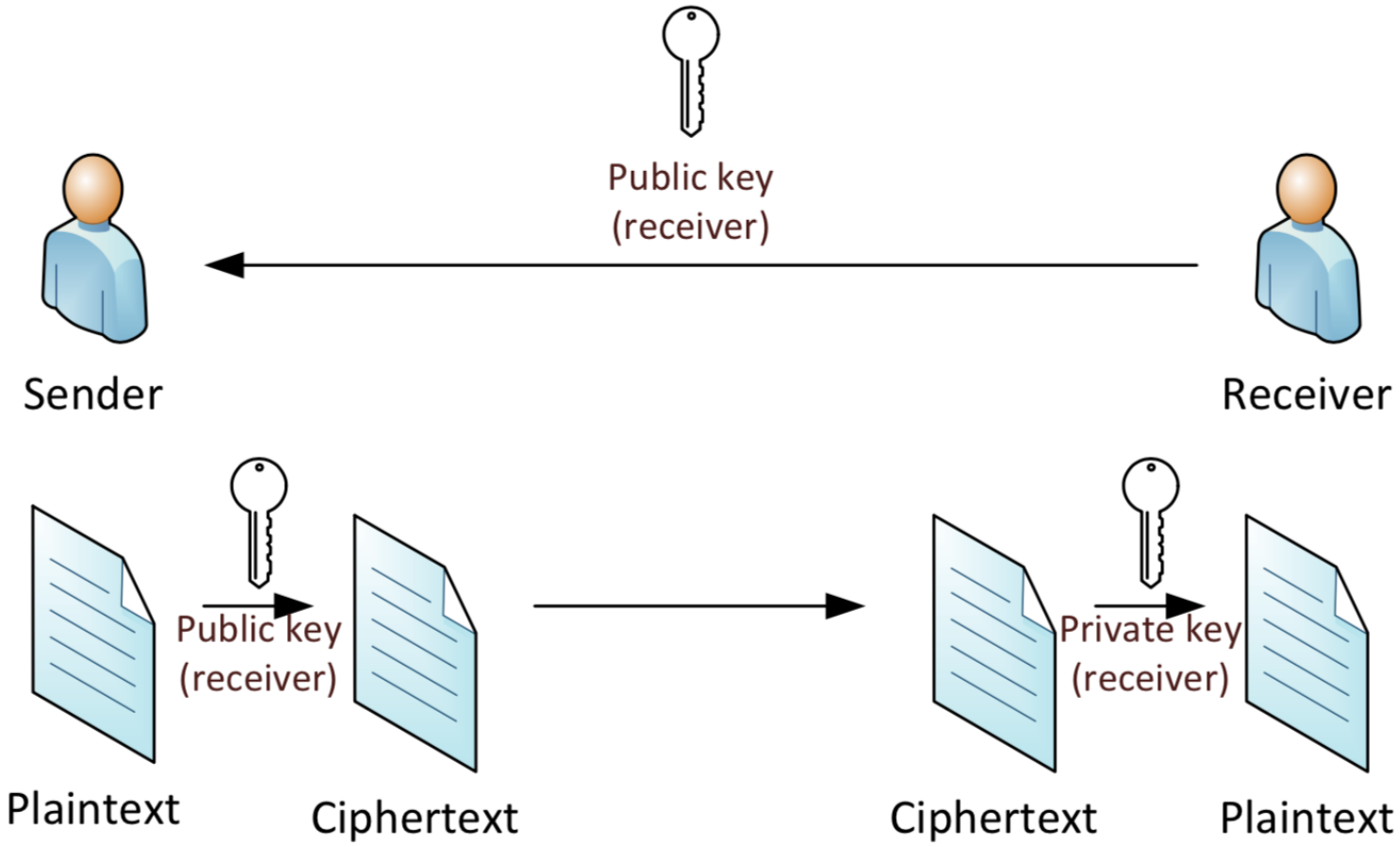
- Sistemas de chave secreta (simétricos) (ou convencionais)
  - A encriptação e a desencriptação são rápidas
  - É difícil distribuir as chaves secretas de forma segura
- Sistemas de chave pública (assimétricos)
  - Mais lentos do que a encriptação por chave secreta
  - Resolvem o problema da distribuição de chaves secretas



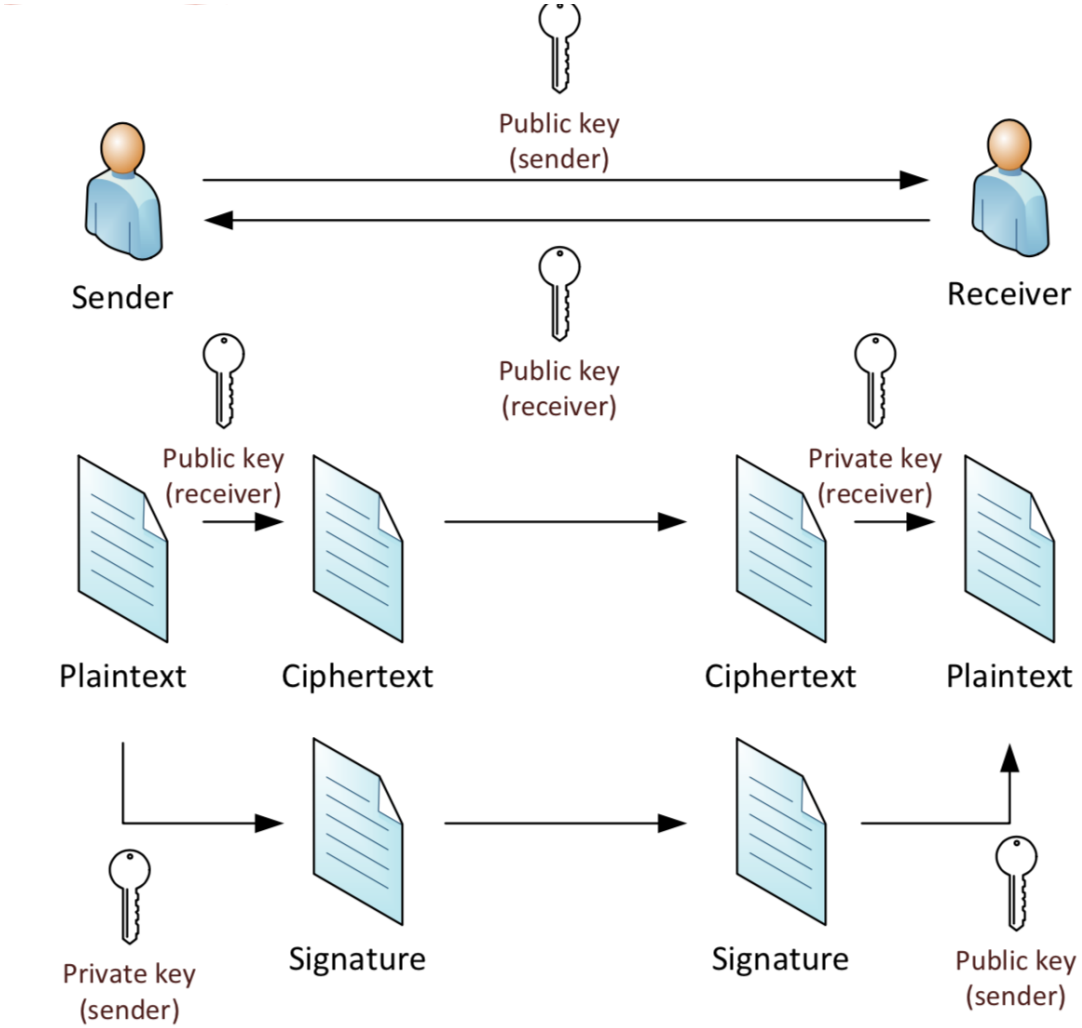
# Confidencialidade com encriptação simétrica



# Confidencialidade com encriptação assimétrica



# Encriptação e assinatura com encriptação assimétrica



# Encriptação com PGP


## Emissor

- Gera uma chave (única) de sessão
- Encripta o *plaintext* com a chave de sessão
- Encripta a chave de sessão com a chave pública de recetor
- Envia o texto encriptado + chave de sessão encriptada

## Recetor

- Utiliza a sua chave privada para desencriptar a chave de sessão
- Com a chave de sessão já consegue desencriptar e obter a mensagem original

# Assinaturas com PGP

## Emissor

- Gera um *message digest* (resumo digital) da mensagem a transmitir
- Encripta o *message digest* com a sua chave privada
- Envia mensagem (que não precisa de estar encriptada) juntamente com o *message digest* encriptado

## Recetor

- Gera um *message digest* (resumo digital) da mensagem recebida
- Desencripta a mensagem recebida com a chave pública do emissor
- Compara: se forem iguais considera-se o emissor autenticado e garante-se não repudiação (do envio)

# PGP Keyrings

Em sistemas UNIX (Linux, BSD, Mac OS X):

```
cd ~/.gnupg/
        pubring.gpg
        secring.gpg
        trustdb.gpg
```

A validação de chaves no Keyring pode ser:

- **Manual:** chaves podem ser assinadas pelo *Ultimately trusted introducer* (o próprio utilizador)
- **Automatic:** se a chave PGP importada já tem assinaturas de *Marginally trusted introducers* em número suficiente