STI
MEI/MIEBIOM

2022/2023

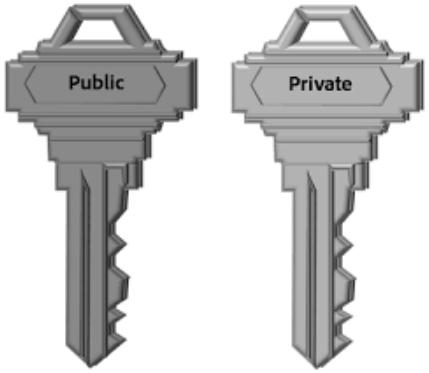
Practical class #1

- PGP (Pretty Good Privacy)

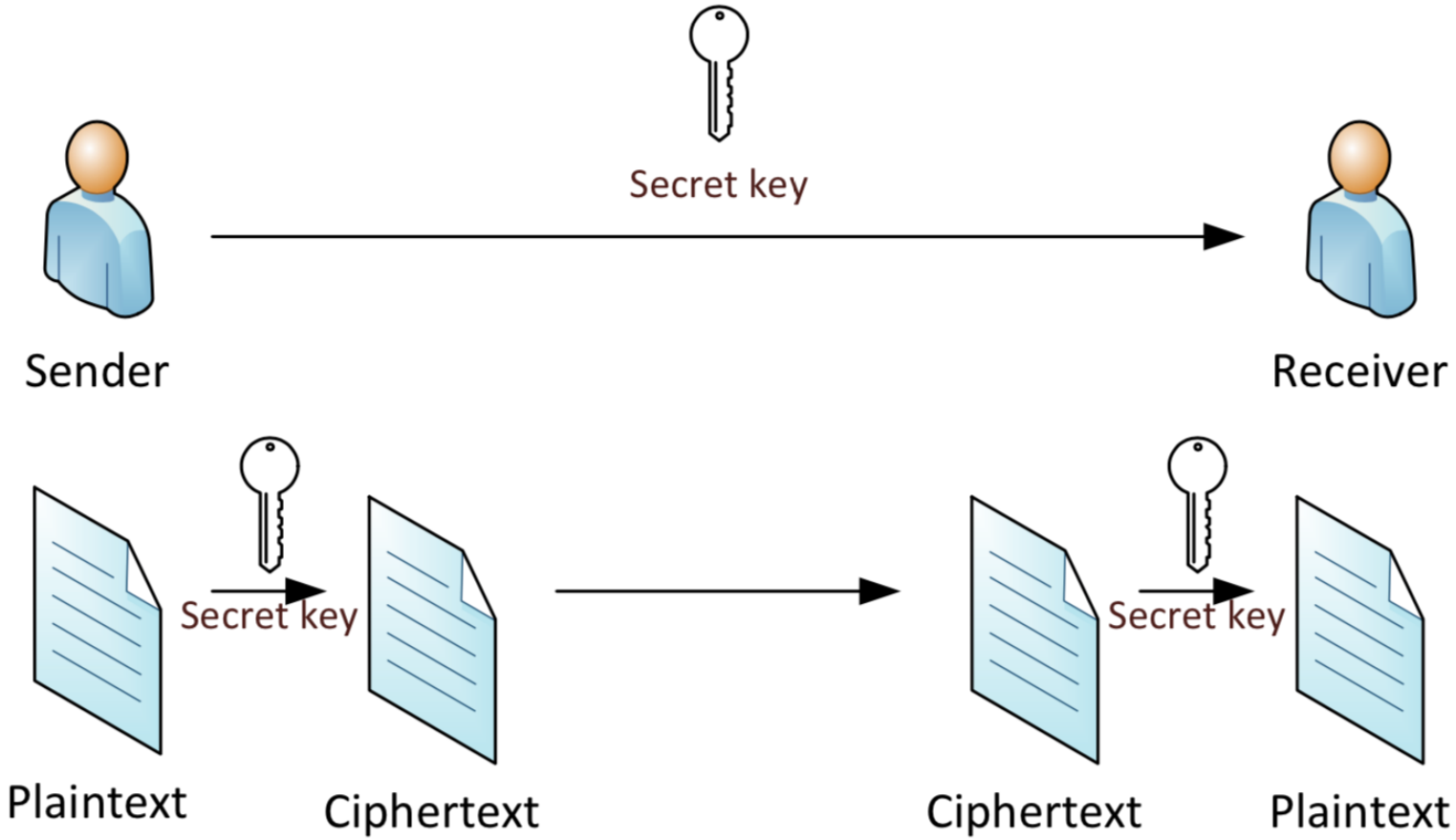
Cryptographic systems

- **Secret-key (symmetric) systems (or conventional)**
  - Encryption and decryption is fast
  - It is difficult to distribute secret keys securely

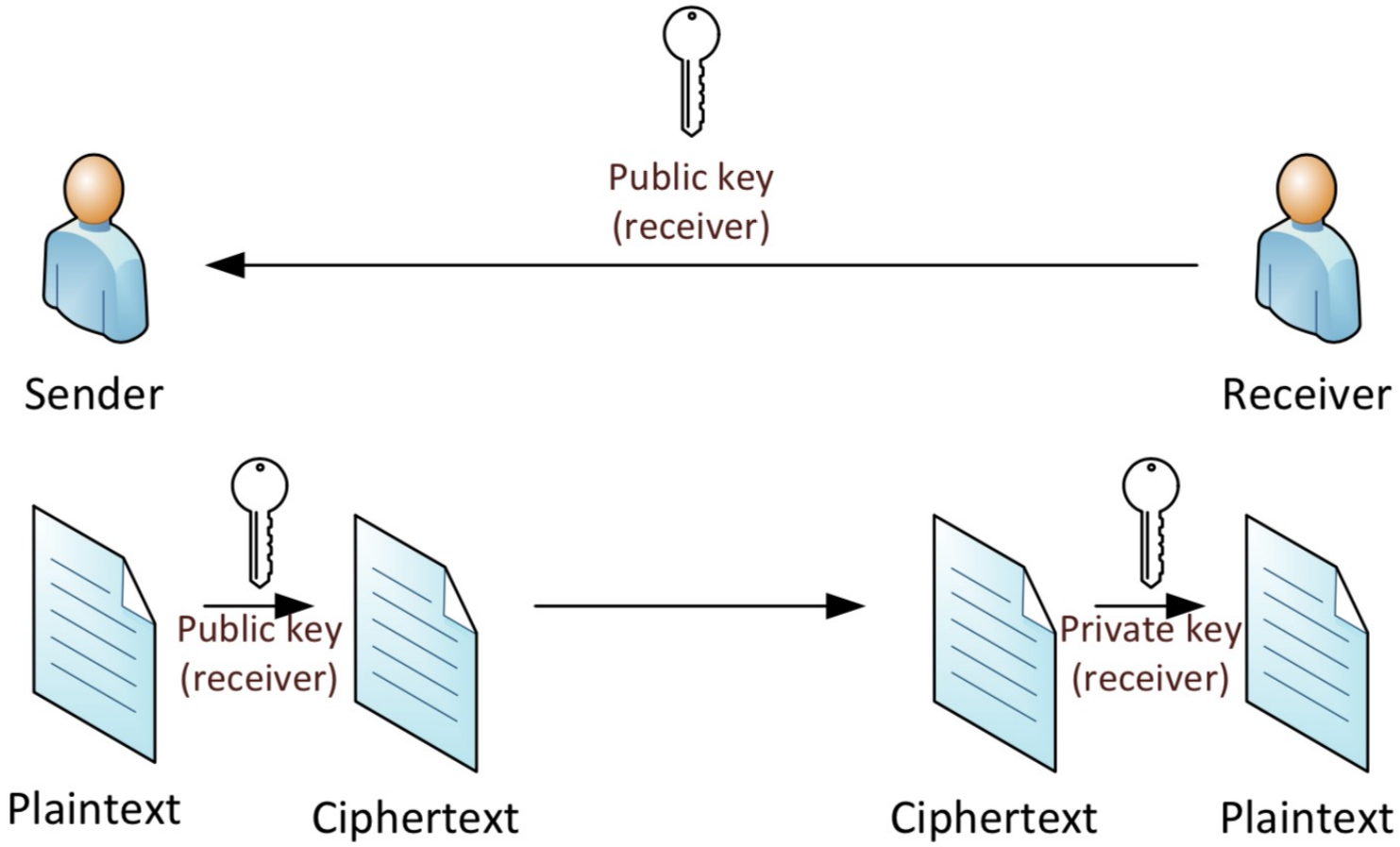
- **Public-key systems, or asymmetric**
  - Slower than secret-key encryption
  - Address the issue of secret key distribution



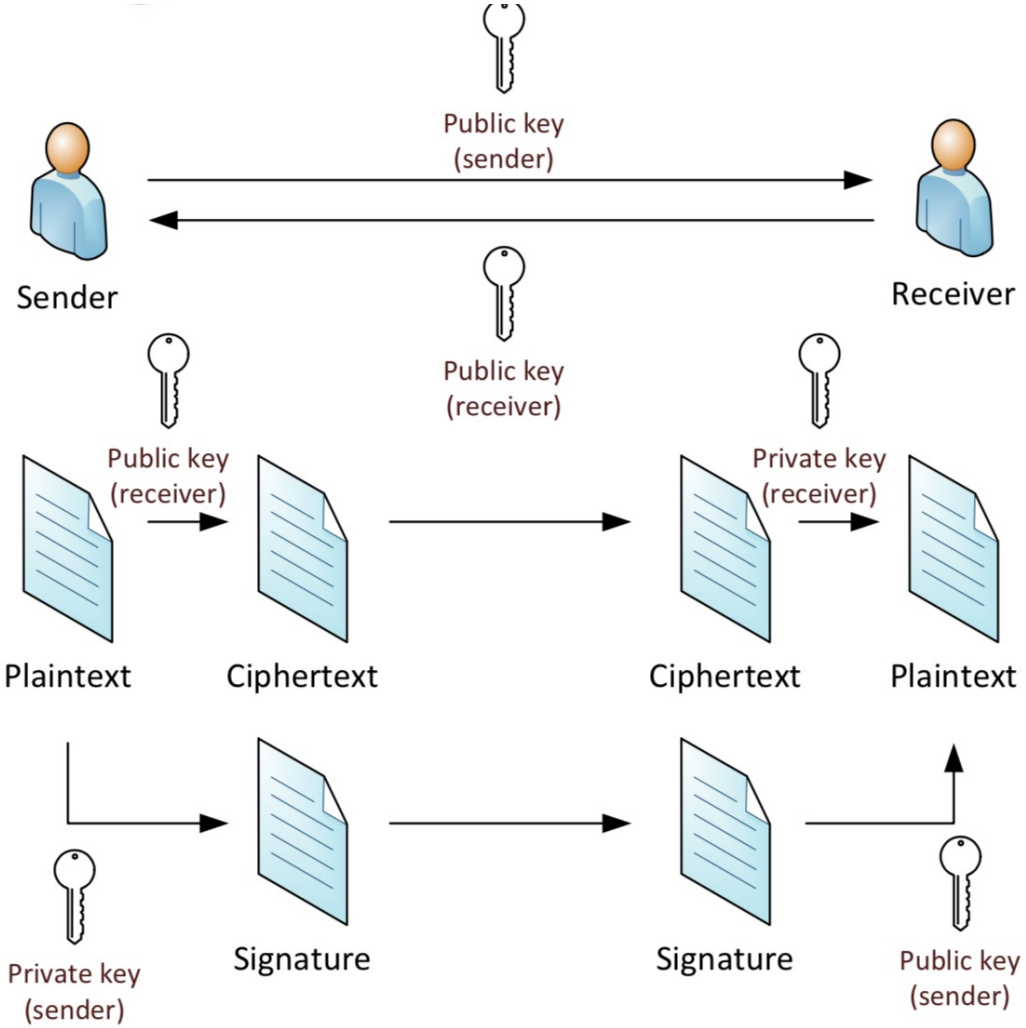
Conventional (symmetric) cryptography (confidentiality)



Asymmetric cryptography (confidentiality)



Asymmetric cryptography (encrypting and signing)



Encrypting with PGP

Sender

- Generate a (unique) session key
- Encrypts plaintext with session key
- Encrypts session key with the receiver's public-key
- Send encrypted text + encrypted session key

Receiver

- Uses its private key to decrypt session key
- Decrypts message using session key

Signing with PGP

Sender

- Generates a *message digest* of the message to transmit
- Encrypts message digest with its private key
- Sends message (may be in clear text) with the encrypted message digest

Receiver

- Generates a message digest of the message received
- Decrypts the received message digest with the sender's public key
- Compares the two

PGP Keyrings

In UNIX systems (Linux, BSD, Mac OS X):

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

Validation of keys in the Keyring:

- **Manual validation** (keys are signed by the *Ultimately trusted introducer*, e.g. you)
- **Automatic validation** (PGP keys already contains enough signatures from *Marginally trusted introducers*)