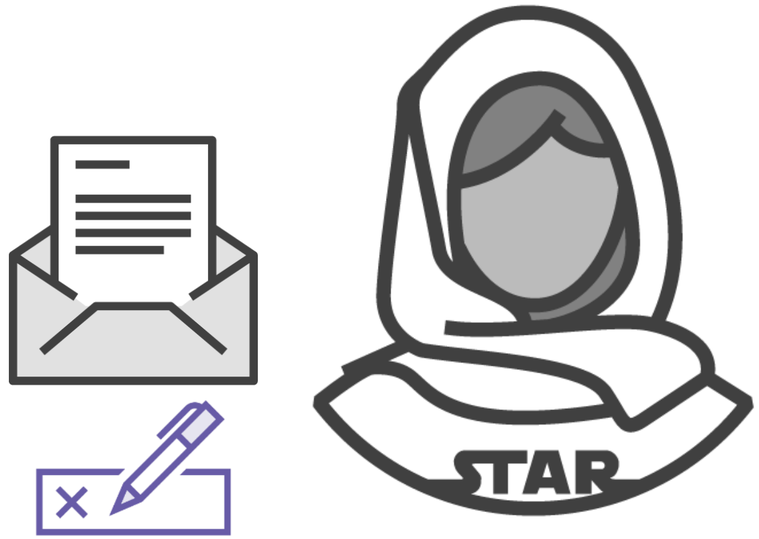
# Outlining Email and Disk Encryption

**Dale Meredith**
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

# Digital Signature




Public Key

Private Key

# Digital Signature


Public Key

Private Key

# Digital Signature

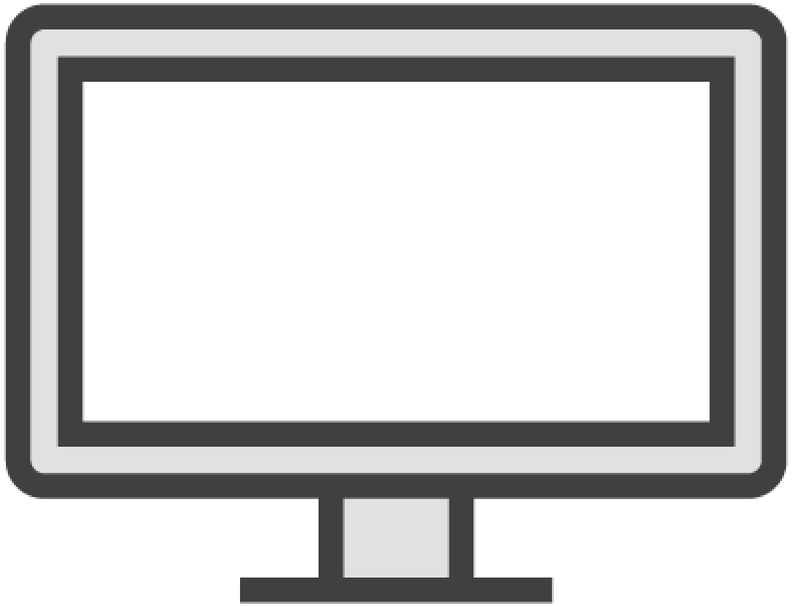

Public Key

Private Key

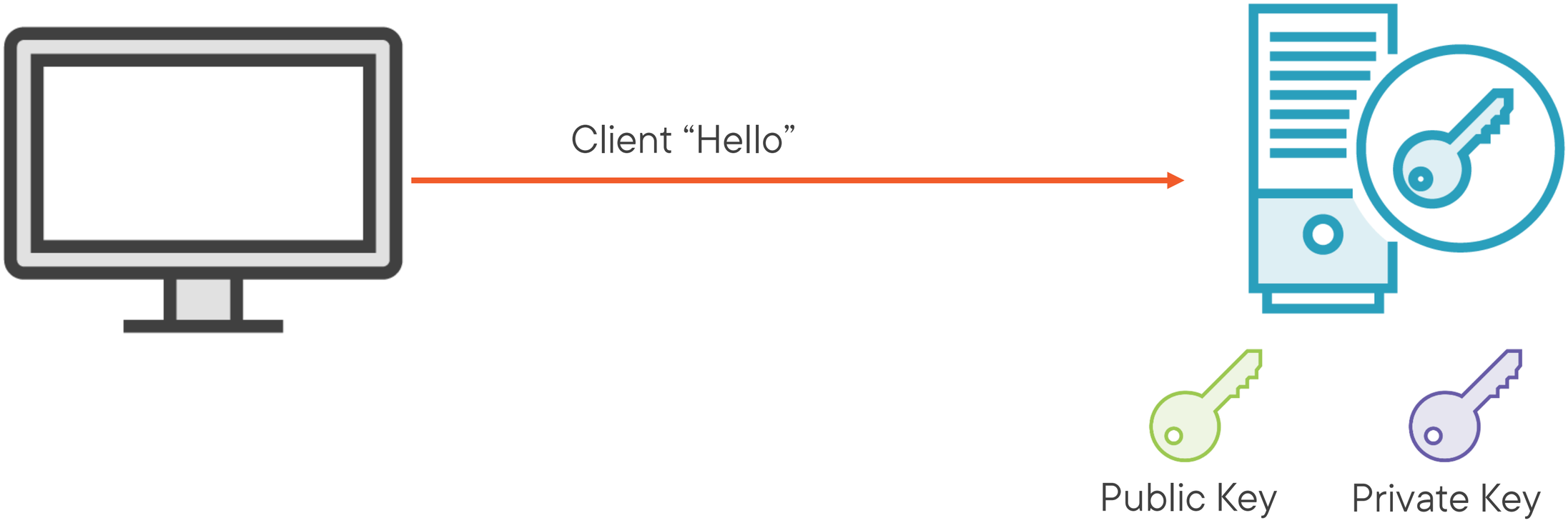
# Secure Socket Layer (SSL) and Transport Layer Security (TLS)

# SSL and TLS

# SSL and TLS

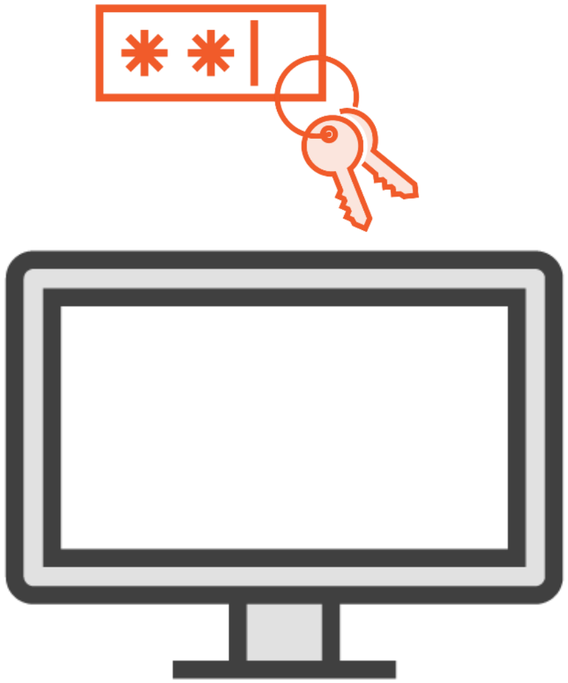


# SSL and TLS



# SSL and TLS

# SSL and TLS

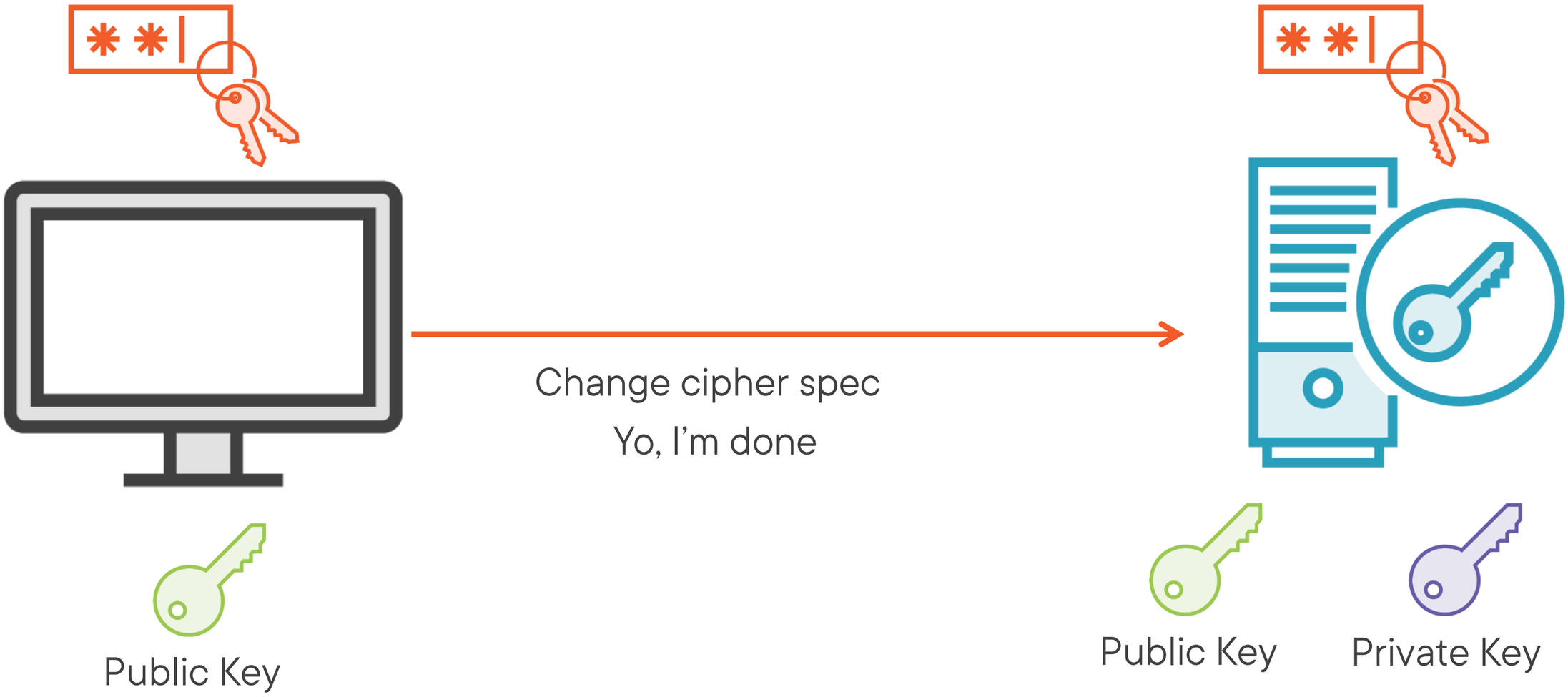


Public Key

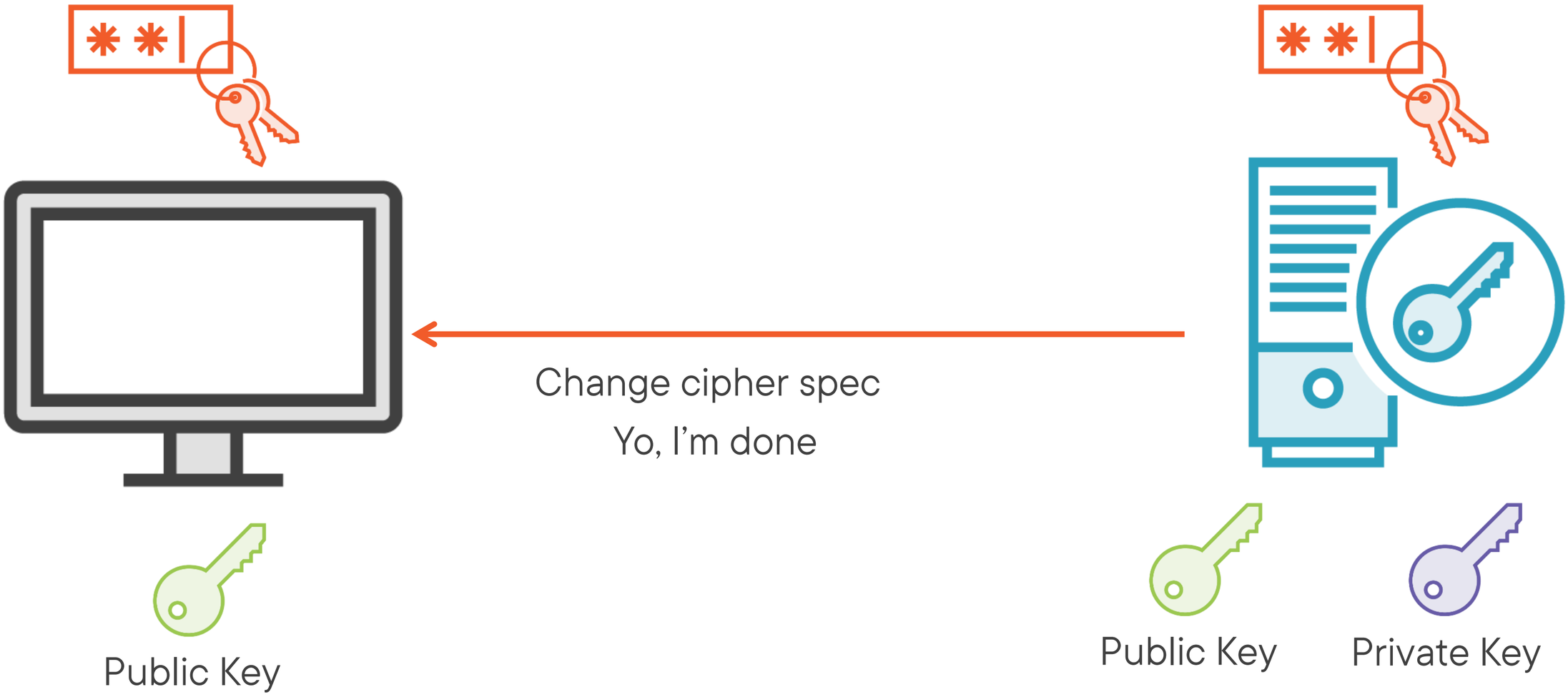
Public Key

Private Key

# SSL and TLS



# SSL and TLS



# SSL and TLS

# OpenSSL

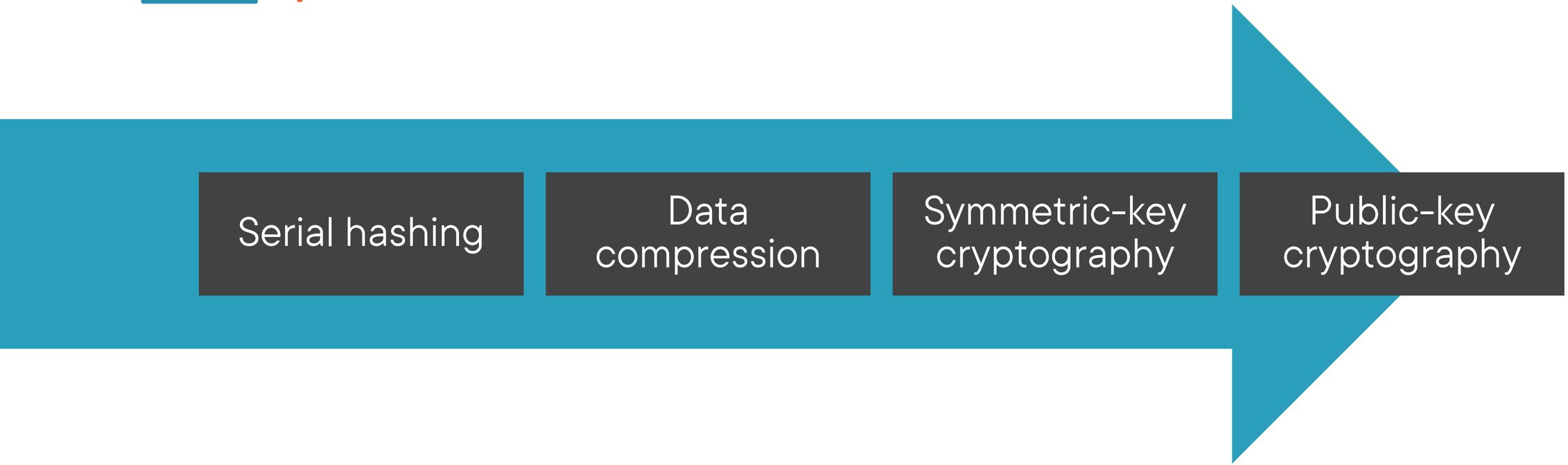
# OpenSSL

# More Email Ciphers

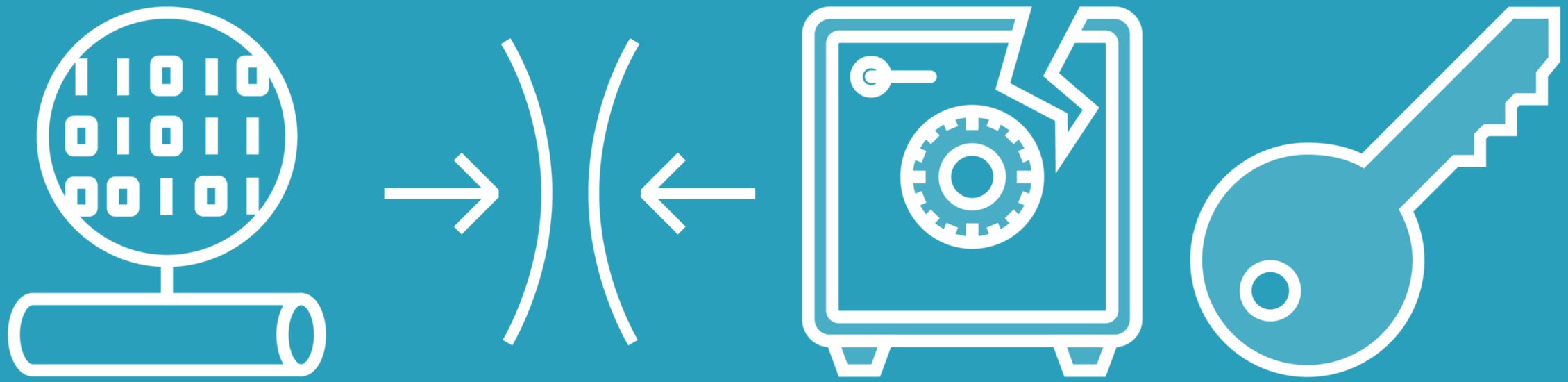
# Pretty Good Privacy (PGP)

**Used to encrypt and decrypt data, files and messages**

**Used for data compression, digital signing and to enhance the privacy of email communications**



# Pretty Good Privacy (PGP)



# GNU Privacy Guard (GPG)

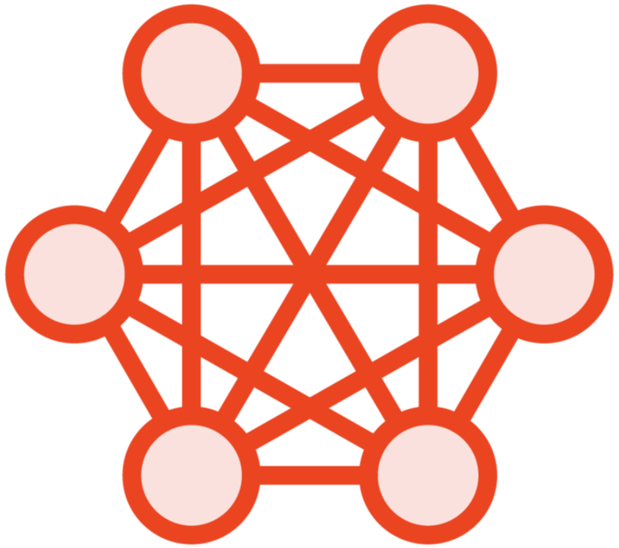
**Hybrid encryption program**

**Allows for increased speed and secure key exchange**

# Web of Trust (WOT)

**A trust model of PGP, OpenPGP, and GnuPG accessible systems**

- **Users decide who to trust**
- **Signatures are verified by others who have that person's public key**
- **The decentralized trust model makes it more difficult to impersonate a user**
- **Used by OTR (Off-the-Record Messaging), TOR and other systems**



# Web of Trust (WOT)

## Strengths

Cryptographic signatures verify messages are being received from a trusted source

Minimizes MiTM attacks

Protects against DoS attacks

## Opportunities

Can be challenging to get enough people to sign your key for it to be considered trustworthy

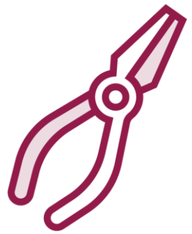
Keys can be revoked if someone's trustworthiness changes

# Demo

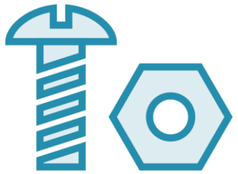
## Using Rmail to Secure Emails

# Disk Encryption

# Disk Encryption Tools



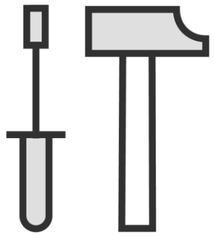
**BitLocker Drive Encryption**



**VeraCrypt**

**BitLocker-to-go**

**FileVault**



**Company IT Policy**

**GNOME Disk Utility**

# Learning Check

# Learning Check

- **Both!**
- **Generates a new master secret and session key**
- **Heartbleed**
- **PGP**
- **Web of Trust (WoT)**

# Up Next: Investigating Cryptanalysis