Applied!

Data & Network Security

Behnam Amiri

ans.dailysec.ir

aNetSec.github.io

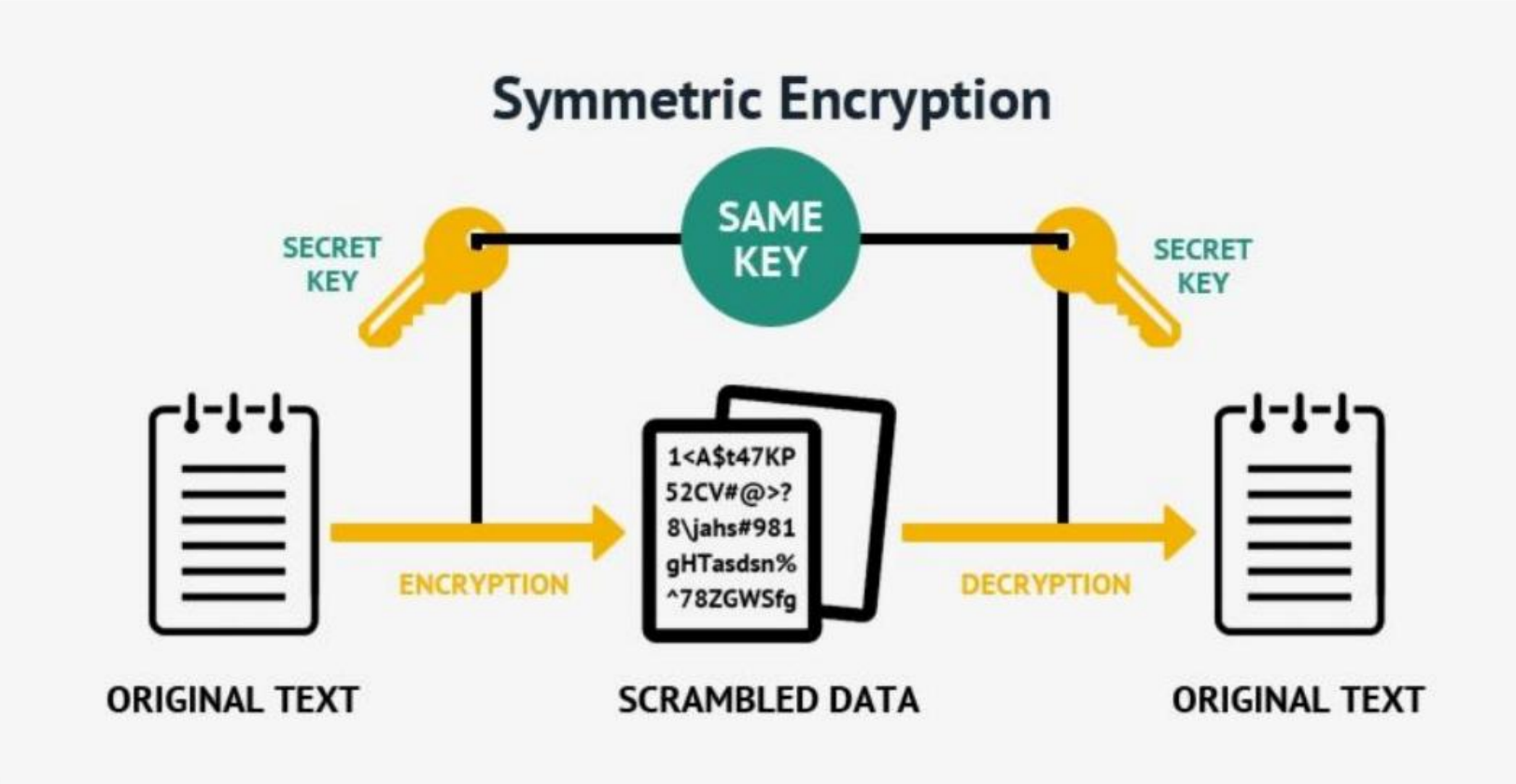
Spring 2025

Recap

CIA Triangle

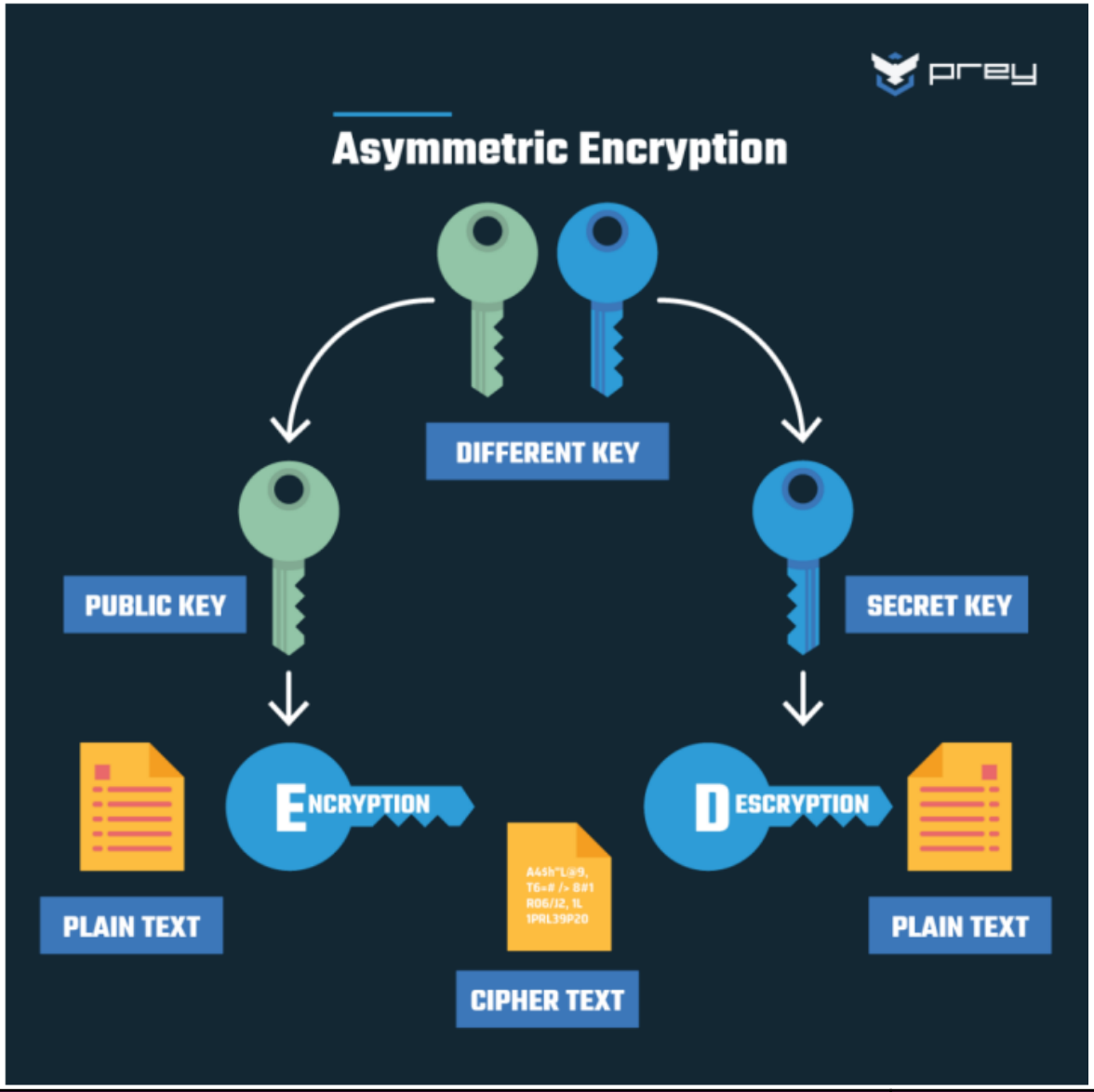
Symmetric encryption

- Same key for Encryption & Decryption



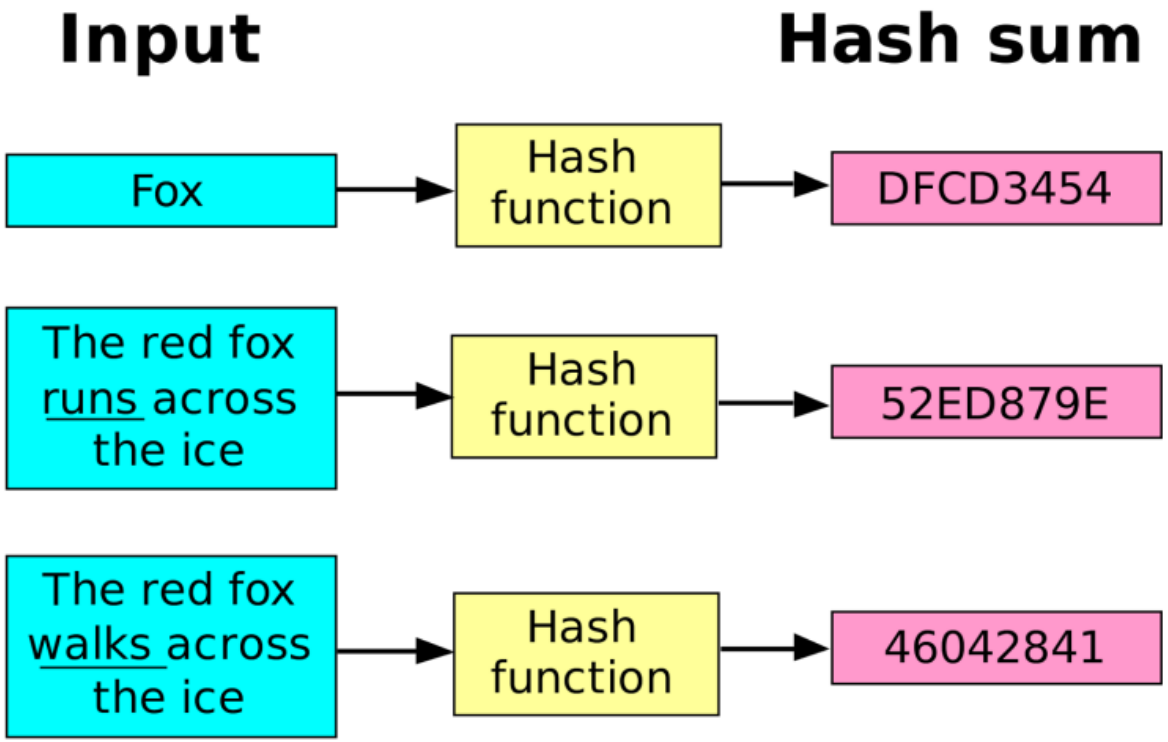
Asymmetric encryption

- Public Key for encryption
- Private Key for decryption



Hash Function

- One-way function
- Map data of arbitrary size to fixed-size values



Digital Signature

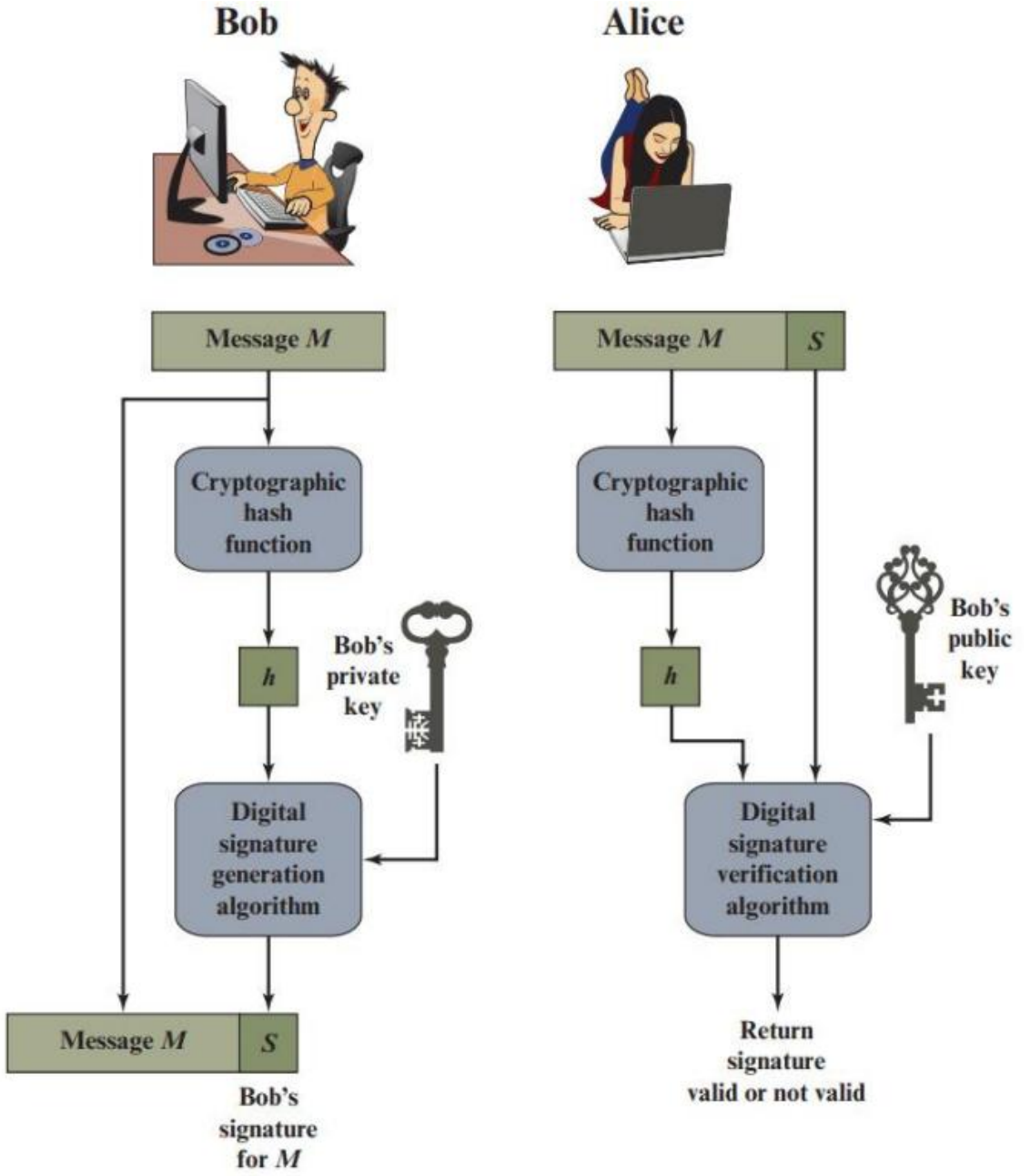


Figure 13.1 Simplified Depiction of Essential Elements of Digital Signature Process

PKI Scenario

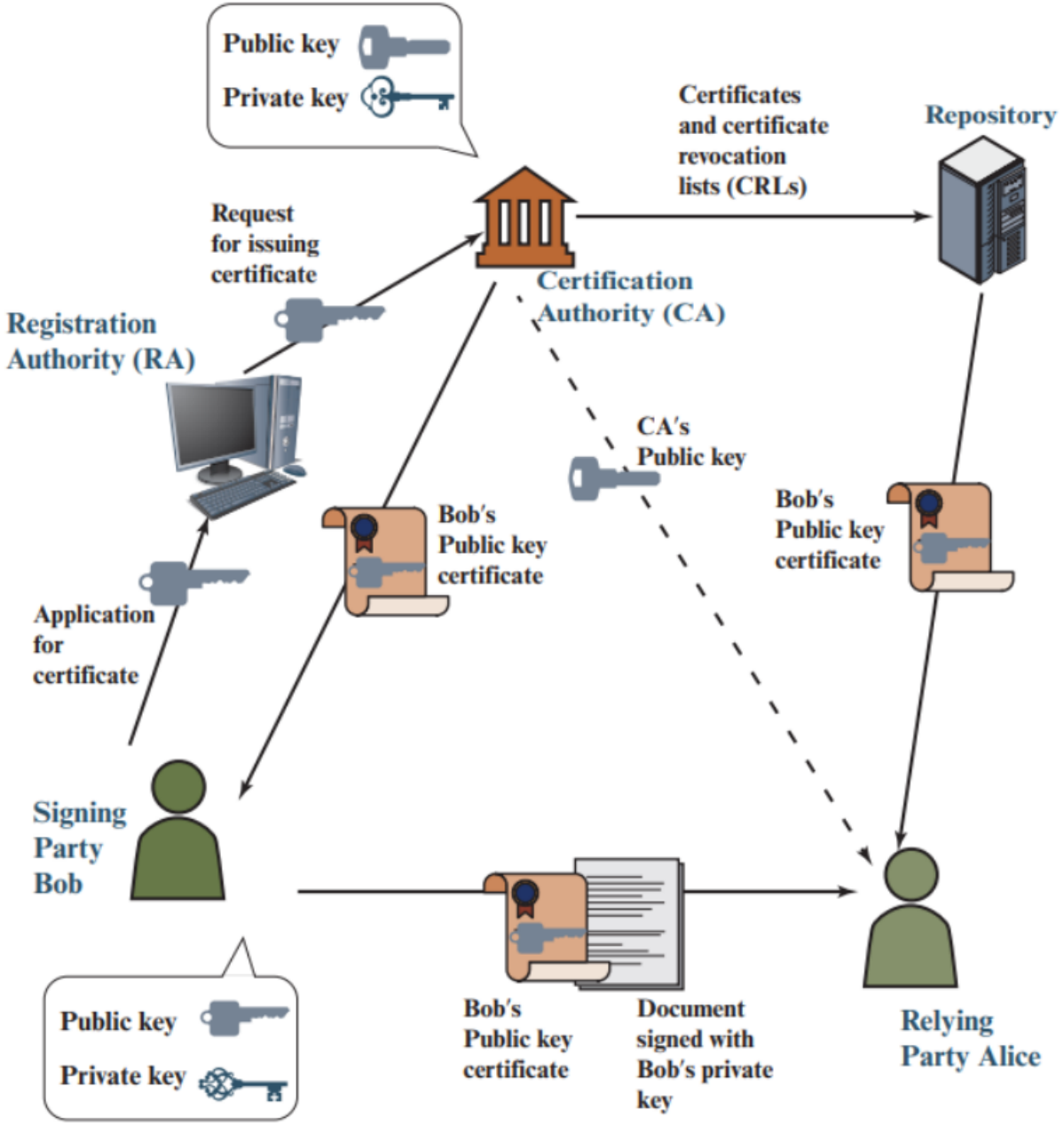
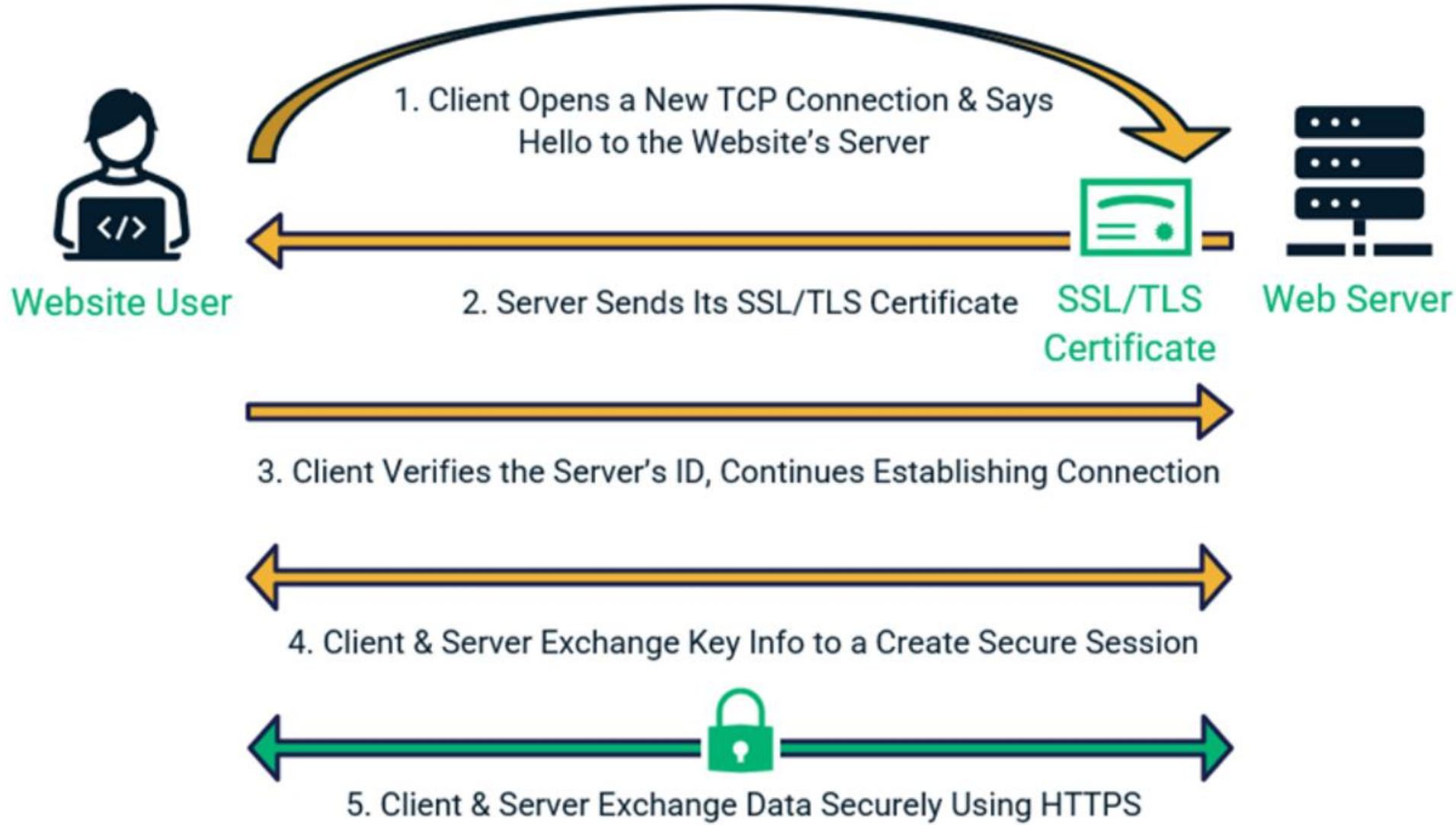


Figure 15.13 PKI Scenario

How PKI Enables Secure Website Connections



PGP

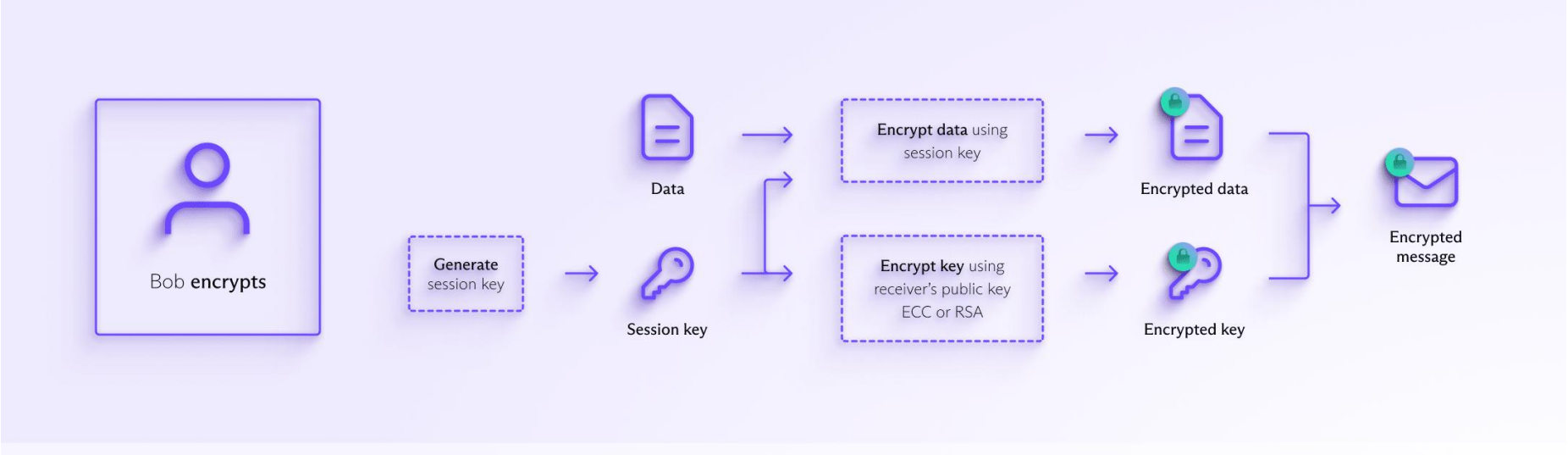
File encryption

- We want encrypt a file and send it via Email.
- Using Symmetric encryption
  - ✓Fast
  - ✓No limit on file size
  - ❖Key share problem!
- Using Asymmetric encryption
  - ✓Public/Private Key is safe.
  - ❖File size limit (file must be smaller than key size)
  - ❖Slow encryption
- ○What we must do?

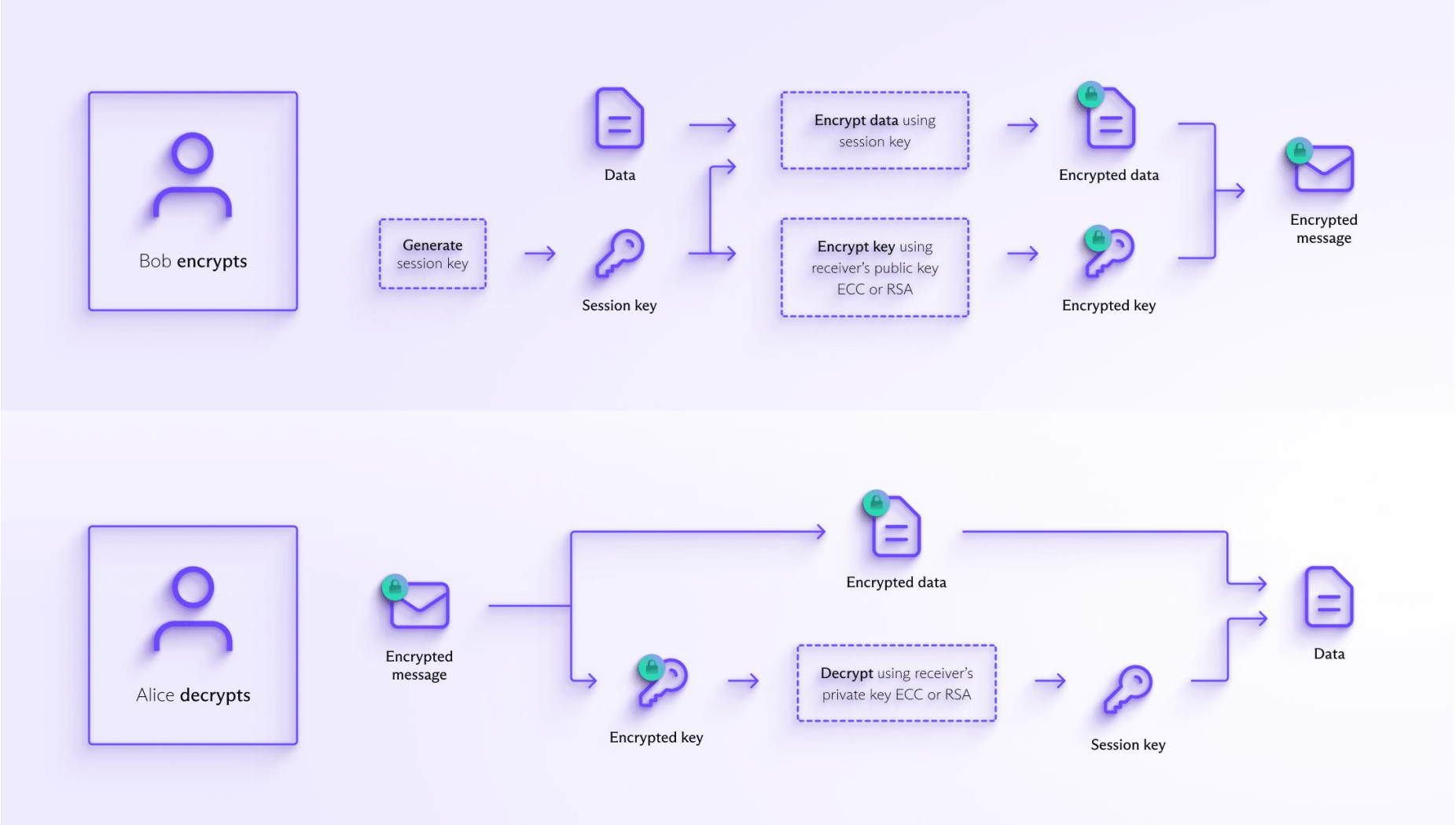
Pretty Good Privacy - PGP

- Generate random symmetric key K1.
- Encrypt file with K1.
- Encrypt K1 with public key.
- Send encrypt file and Encrypted K1 to receiver.

PGP Process


Bob encrypts
Generate session key
Data
Session key
Encrypt data using session key
Encrypt key using receiver's public key ECC or RSA
Encrypted data
Encrypted key
Encrypted message

PGP Process


Bob encrypts
Generate session key
Session key
Data
Encrypt data using session key
Encrypt key using receiver's public key ECC or RSA
Encrypted data
Encrypted key
Encrypted message
Alice decrypts
Encrypted message
Encrypted key
Encrypted data
Decrypt using receiver's private key ECC or RSA
Session key
Data

AmnRo

- AmnRo (امن رو) is a PGP encryption tool.
- https://github.com/amnban/amnro

PGP key distribution

- Give key directly to sender.
- Use public servers like:
  - https://pgp.mit.edu/

PGP History

- Develop by Phil Zimmermann in 1991.
- OpenPGP standard (RFC 4880).
- No longer classified as a non-exportable weapon!

How PGP encryption works visually