Public Key Infrastructure (PKI)

MIH-CPP

PKI

- An infrastructure that uses public key or asymmetric cryptography involving the use of two keys:
  - a public-key, which may be known by anybody, and can be used to encrypt messages, and verify signatures
  - a related private-key, known only to the recipient, used to decrypt messages, and sign (create) signatures
- Infeasible to determine private key from public
- Is asymmetric because
  - two different keys

PKI Guarantees

- Supports:
  - encryption/decryption (provide confidentiality)
  - digital signatures (provide authentication)
  - key exchange (of session keys)
- Some algorithms are suitable for all uses, others are specific to one

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

Confidentiality through PKC

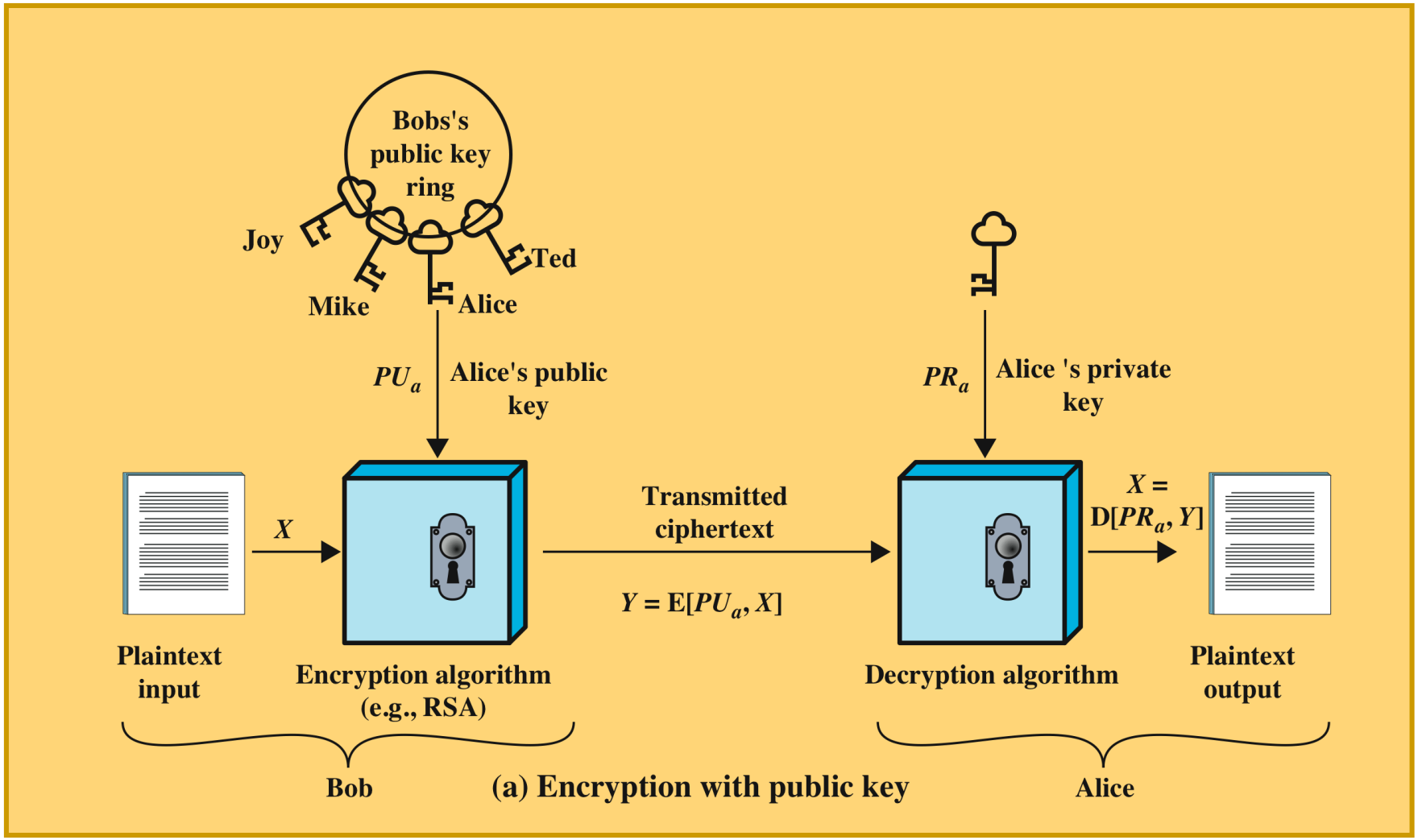


Image Source: Cryptography and Network Security by William Stallings

Authentication through PKC

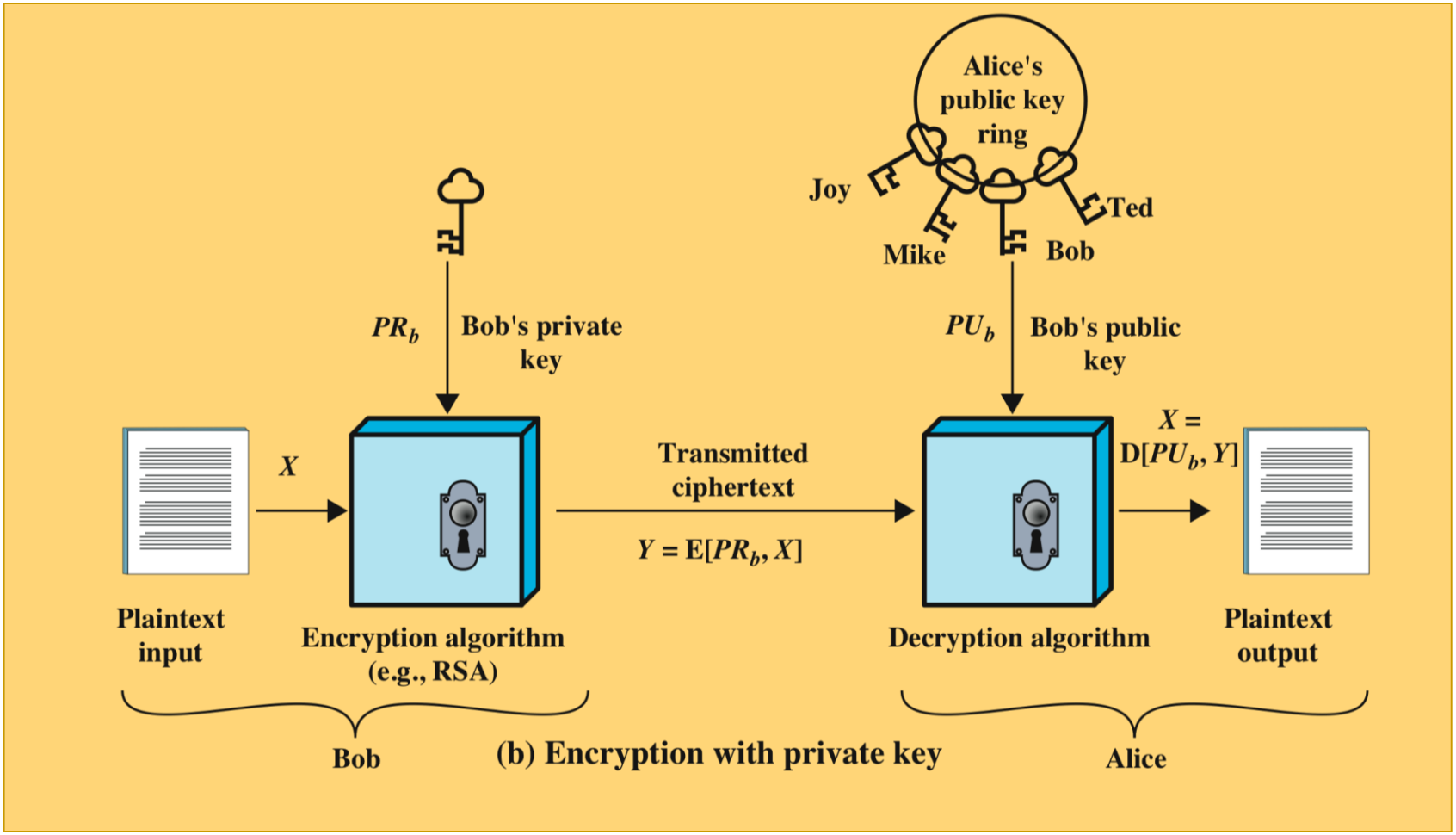
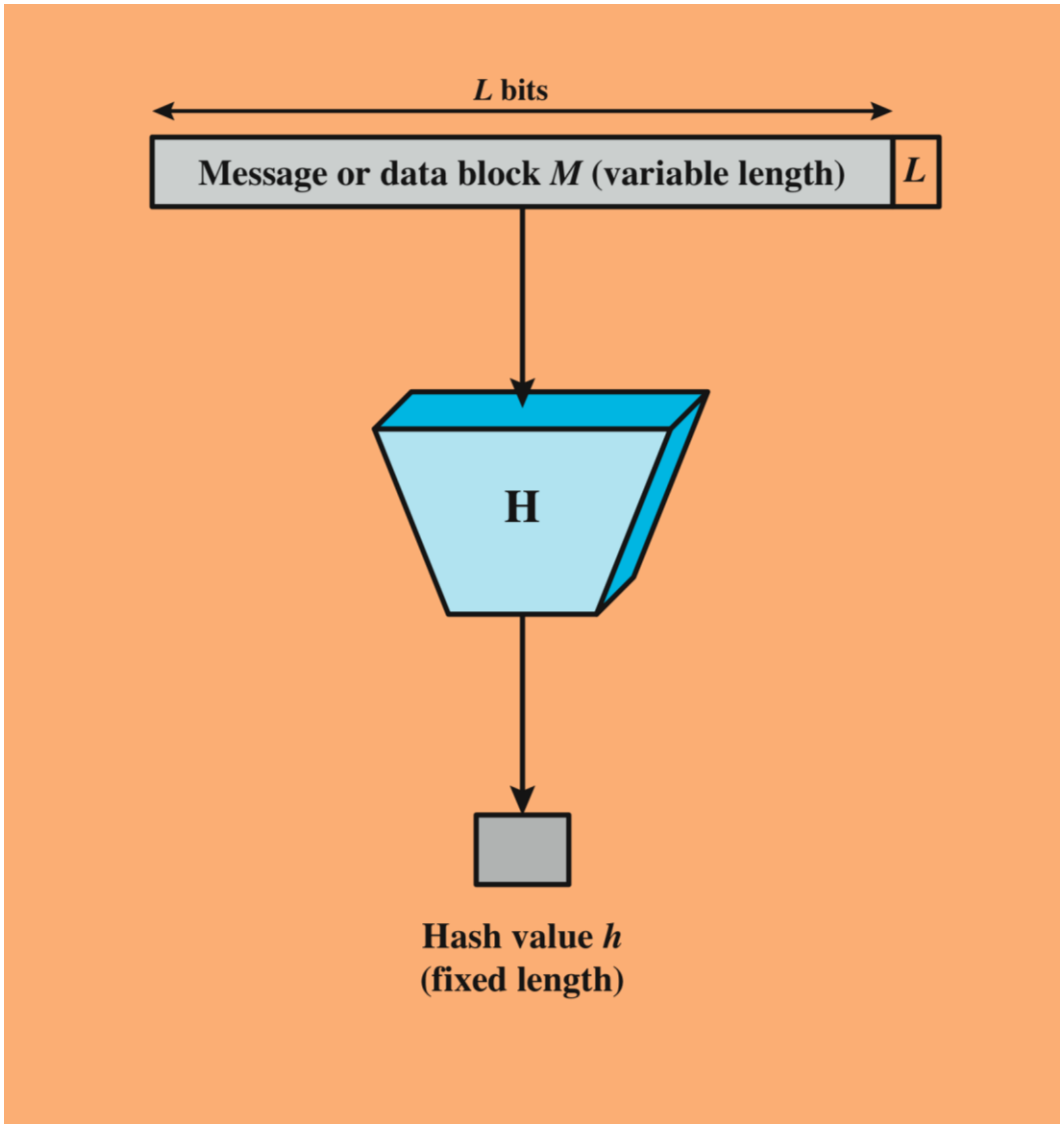


Image Source: Cryptography and Network Security by William Stallings

Hash Functions



MD5 or SHA256

- computationally infeasible to find data mapping to specific hash (one-way property)
- computationally infeasible to find two data to same hash (collision-free property)

Image Source: Cryptography and Network Security by William Stallings

Hash Functions & Digital Signatures

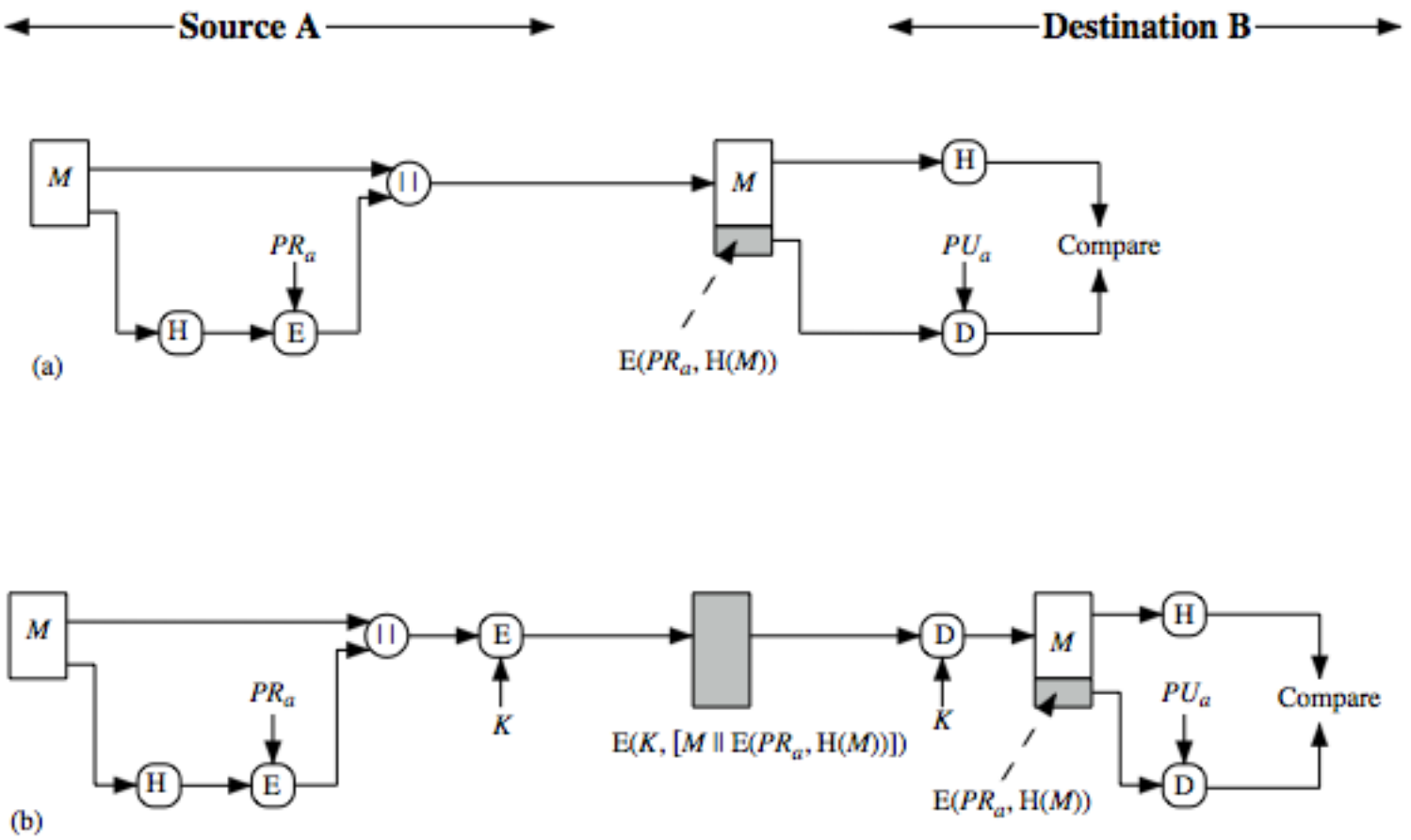
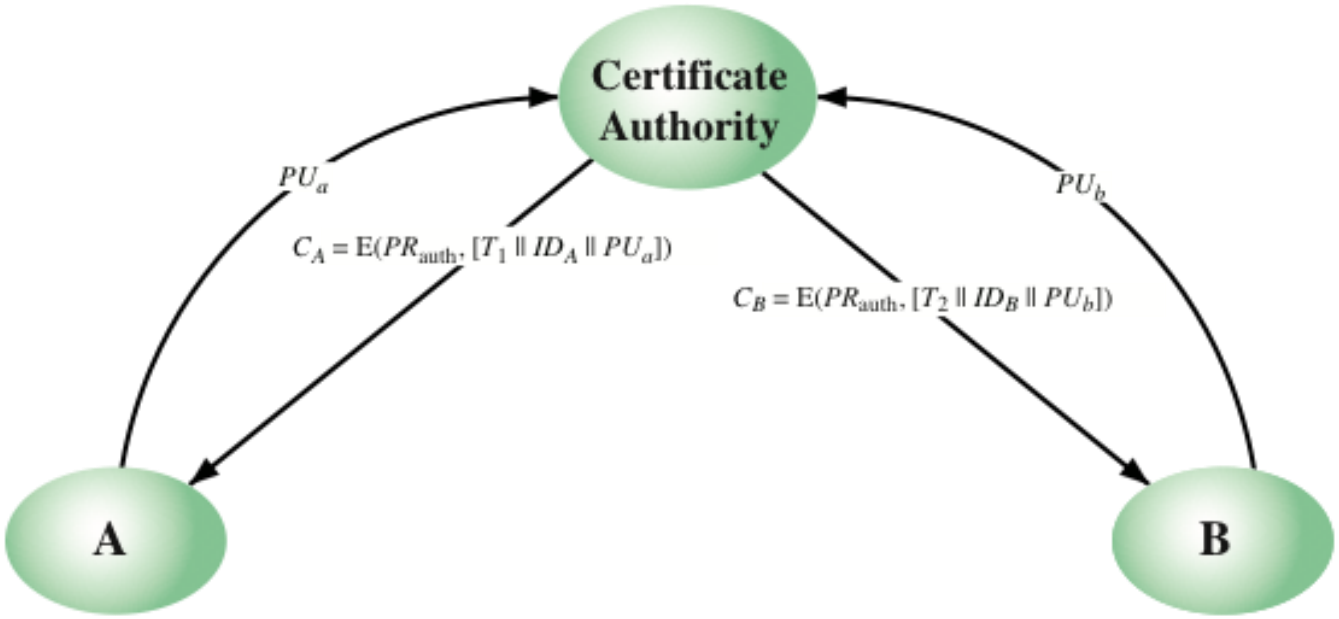
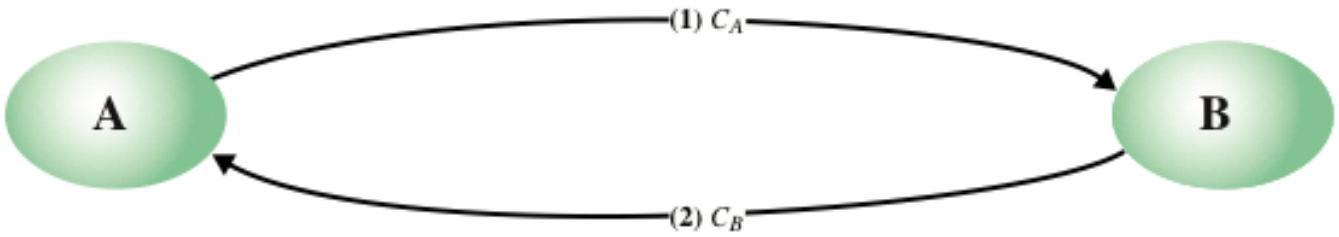


Image Source: Cryptography and Network Security by William Stallings



(a) Obtaining certificates from CA



(b) Exchanging certificates

Image Source: Cryptography and Network Security by William Stallings

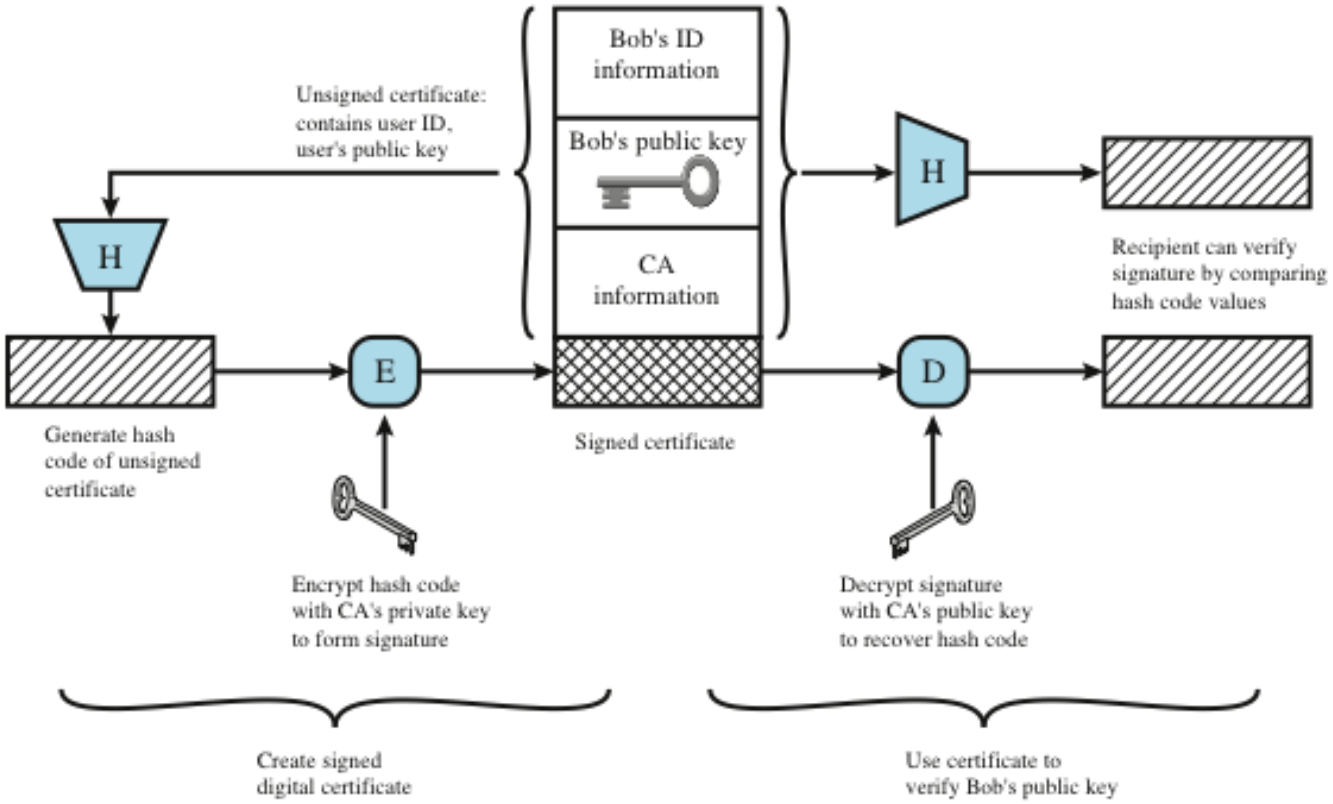


Image Source: Cryptography and Network Security by William Stallings