Digital Signature

- Electronic Transaction Act, 2063
  - Definition
  - Provision on Digital Signature
- Electronic Transaction Rules, 2064

Digital Signature

- A digital signature uses a pair of private-public keys.
- Process
  - A digital signature needs a public-key system. The signer signs with her private key; the verifier verifies with the signer's public key.
  - A cryptosystem uses the public and private keys of the receiver;
    a digital signature uses the private and public keys of the sender.
- Signing the whole document
- Signing the digest
- Services – Integrity, Authentication, Nonrepudiation

Figure Message security

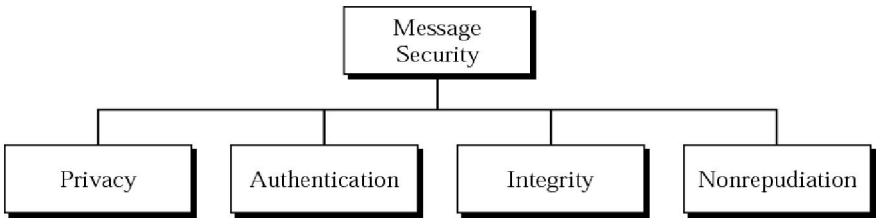


Figure *Digital signature process*

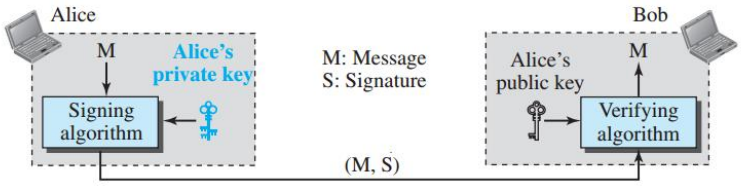


Figure *Signing the digest*

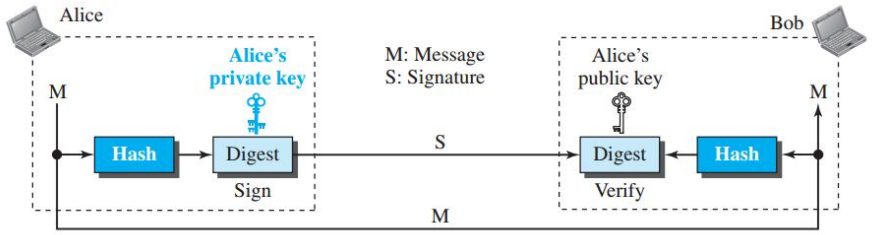


Figure *Using a trusted center for nonrepudiation*

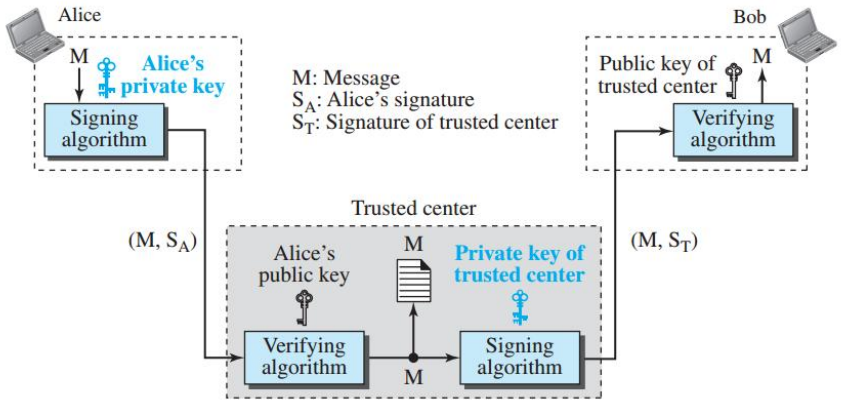


Figure *The RSA signature on the message digest*

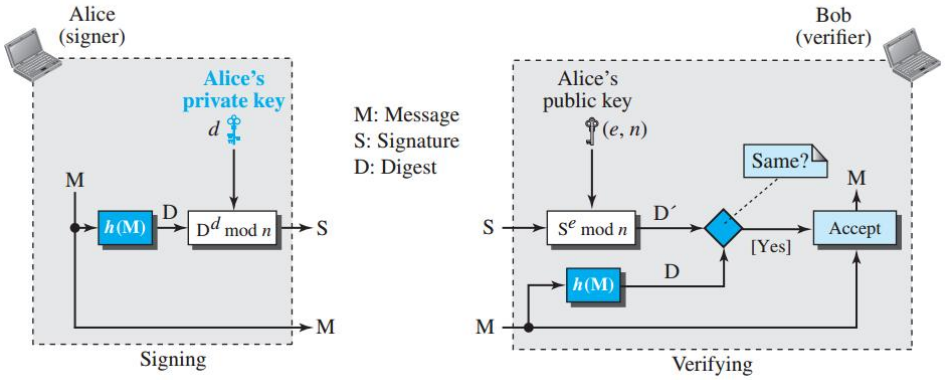


Figure *Unidirectional, symmetric-key authentication*

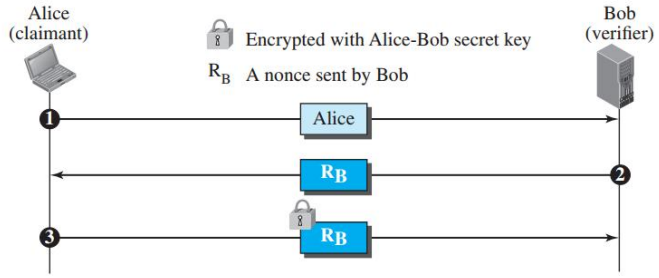


Figure *Unidirectional, asymmetric-key authentication*

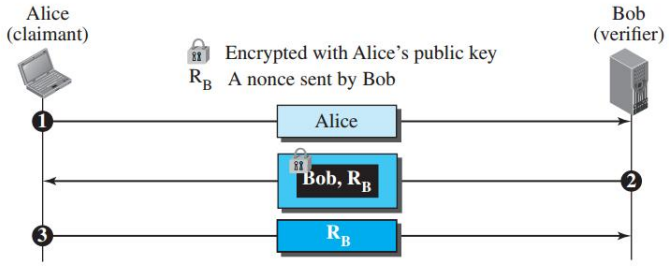
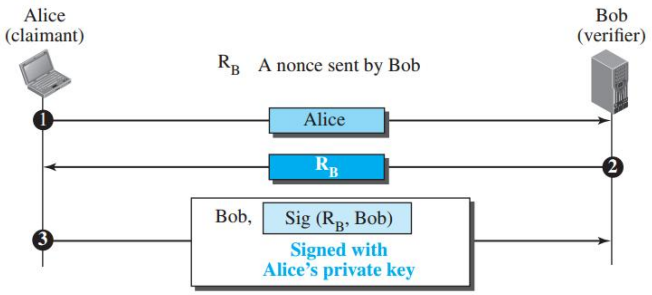


Figure *Digital signature, unidirectional authentication*



Key Management

- Symmetric Key Distribution
- Public Key Distribution
- X.509

Figure *Creating a session key using KDC*

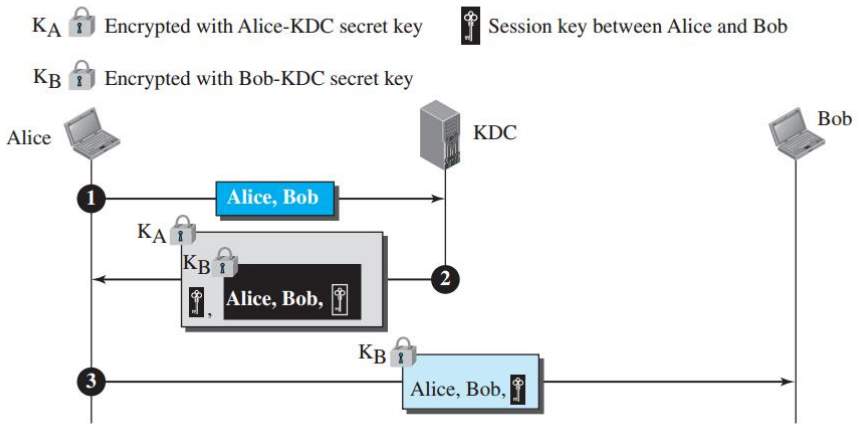


Figure *Certification authority*