Aqsa Khalid
Lecturer
School of Computing

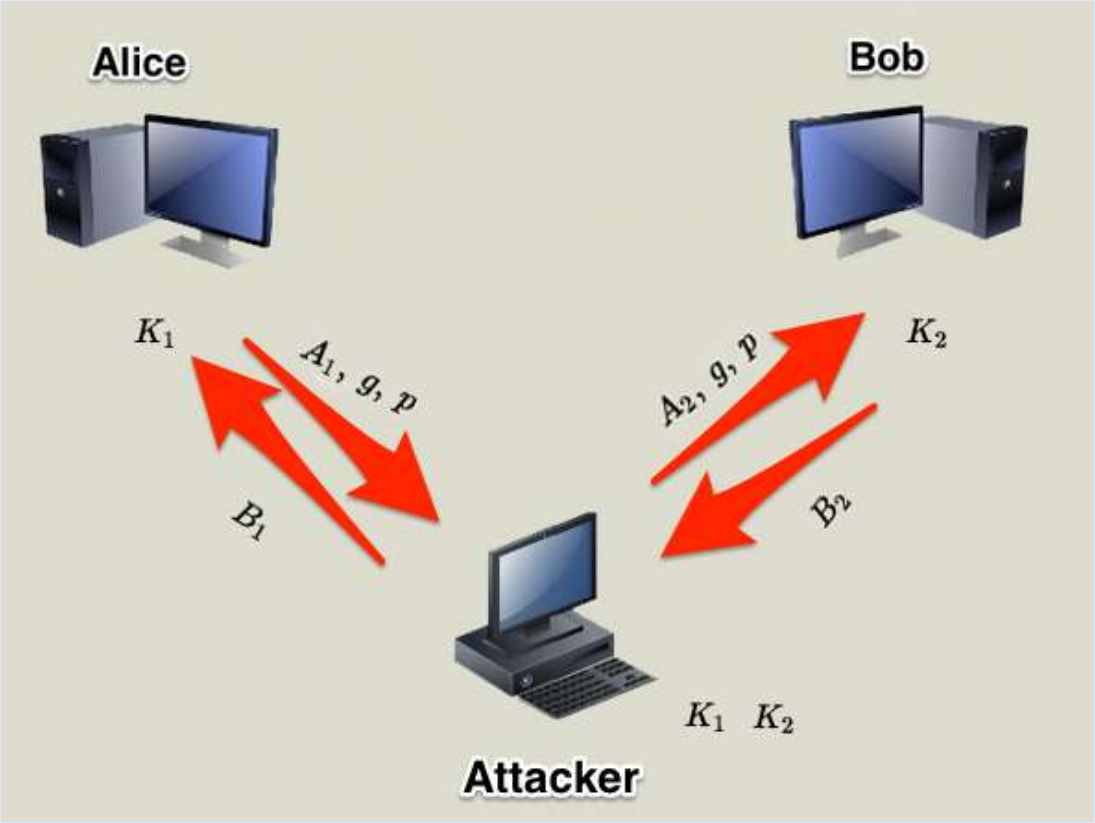
CS3002 Information Security

Asymmetric Cryptography

Source: Stallings chap 2

MITM against Diffie-Hellman

- Vulnerable to main in the middle attack



MITM in PKC

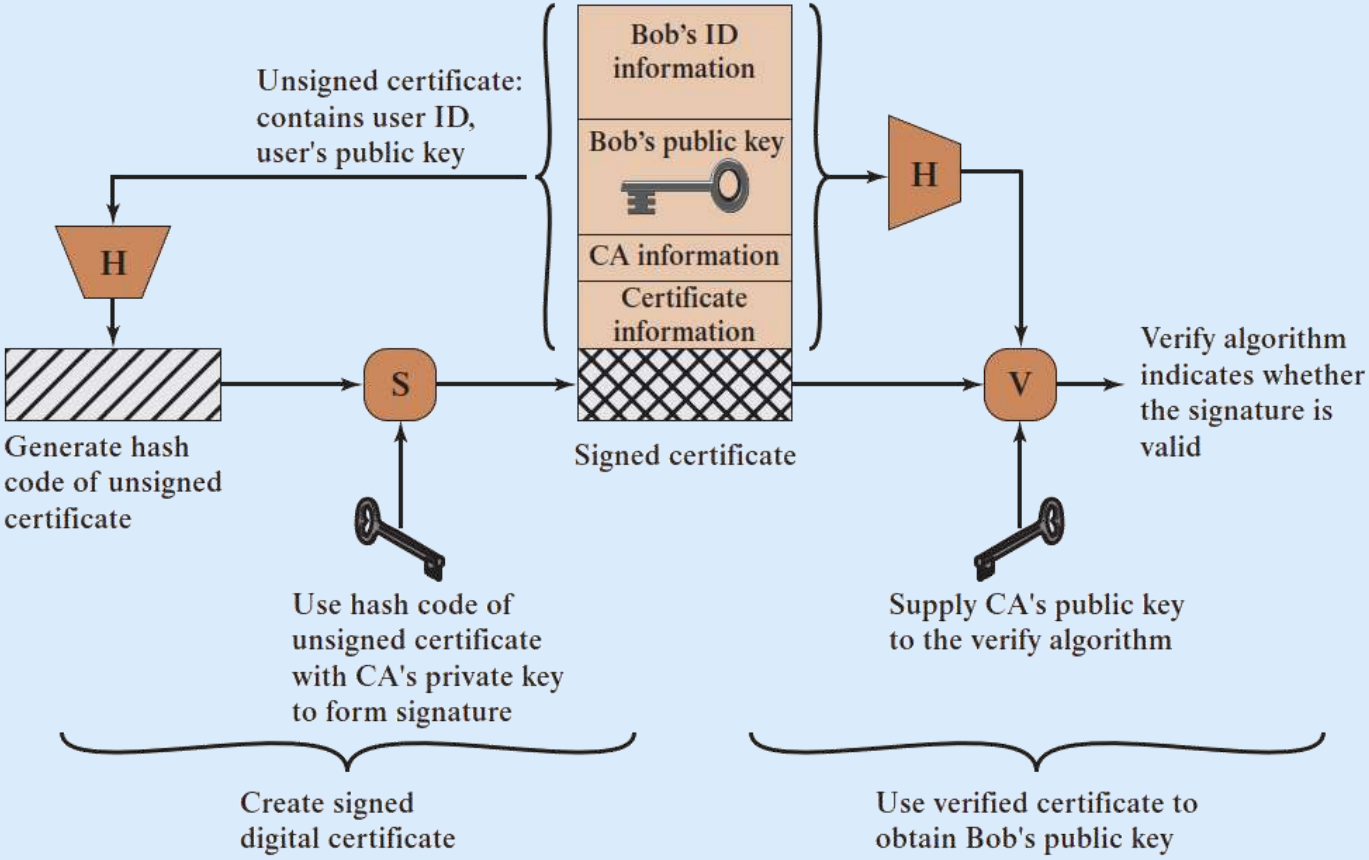
- MITM is not unique to Diffie-Hellman key exchange
- All kinds of asymmetric crypto (RSA, digital signatures, digital envelope etc.) is vulnerable to such attacks
- Whenever public keys are exchanged over an insecure channel, we can not blindly trust the received public key.

Public-Key Certificates

- To prevent MITM against PKC, digital certificates are used.
- A certificate associates a public key with an individual/company
- Digital certificate is just a piece of data
  - A public key and ID of key owner, whole block signed by a **trusted third party**
- Issued by a Certificate Authority (CA)
- Helps in authentication

Public-Key Certificate

- Signing a certificate by CA



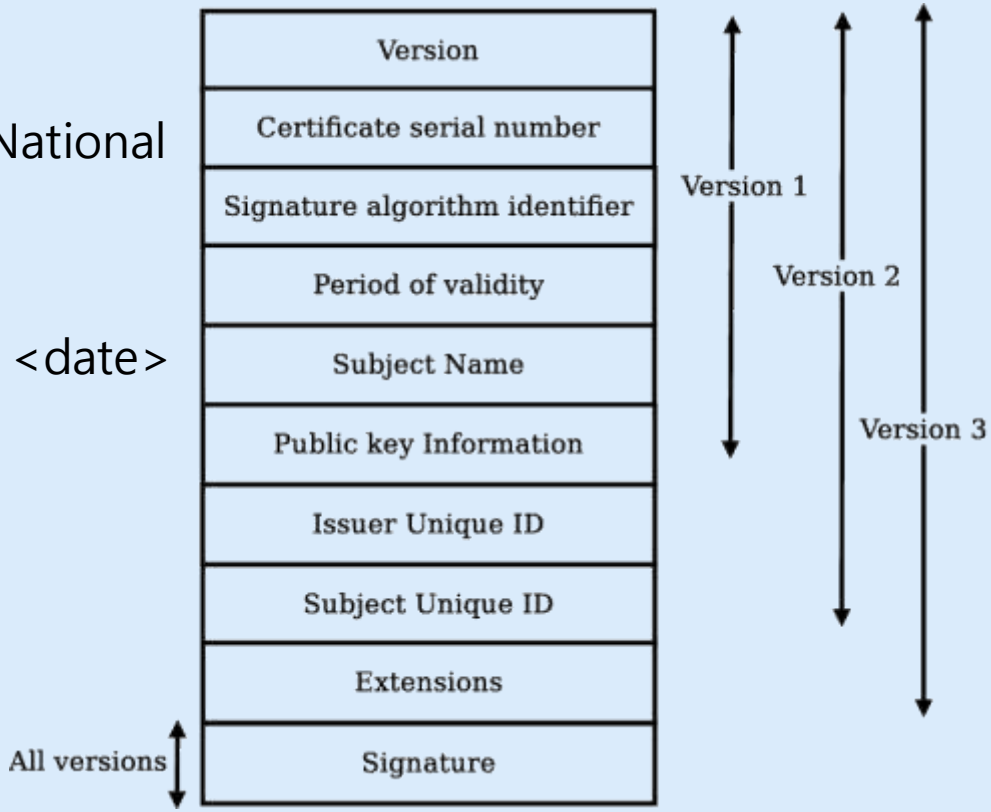
Public-Key Certificate

- Contains the following information:
  - who issued the certificate: Comodo, Symantec etc.
  - who the certificate is issued to
  - public key of the owner
  - validity period
  - digital signature by CA

- X.509: International Standard for the format of a public-key certificate

X.509 Identity Certificates

- Distinguished Name of user
  - C=US, O=Lawrence Berkeley National Laboratory, OU=DSD, CN=Mary R. Thompson
- DN of Issuer
  - C=US, O=Lawrence Berkeley National Laboratory, CN=LBNL-CA
- Validity dates:
  - Not before <date>, Not after <date>
- User's public key
- V3 extensions
- CA signatures
- Defined in ASN.1 notation
  - language independent



Public Key Infrastructure

Public Key Infrastructure (PKI)

- Set of hardware, software, and procedures needed to create, store, distribute and revoke digital certificates

Elements of PKI

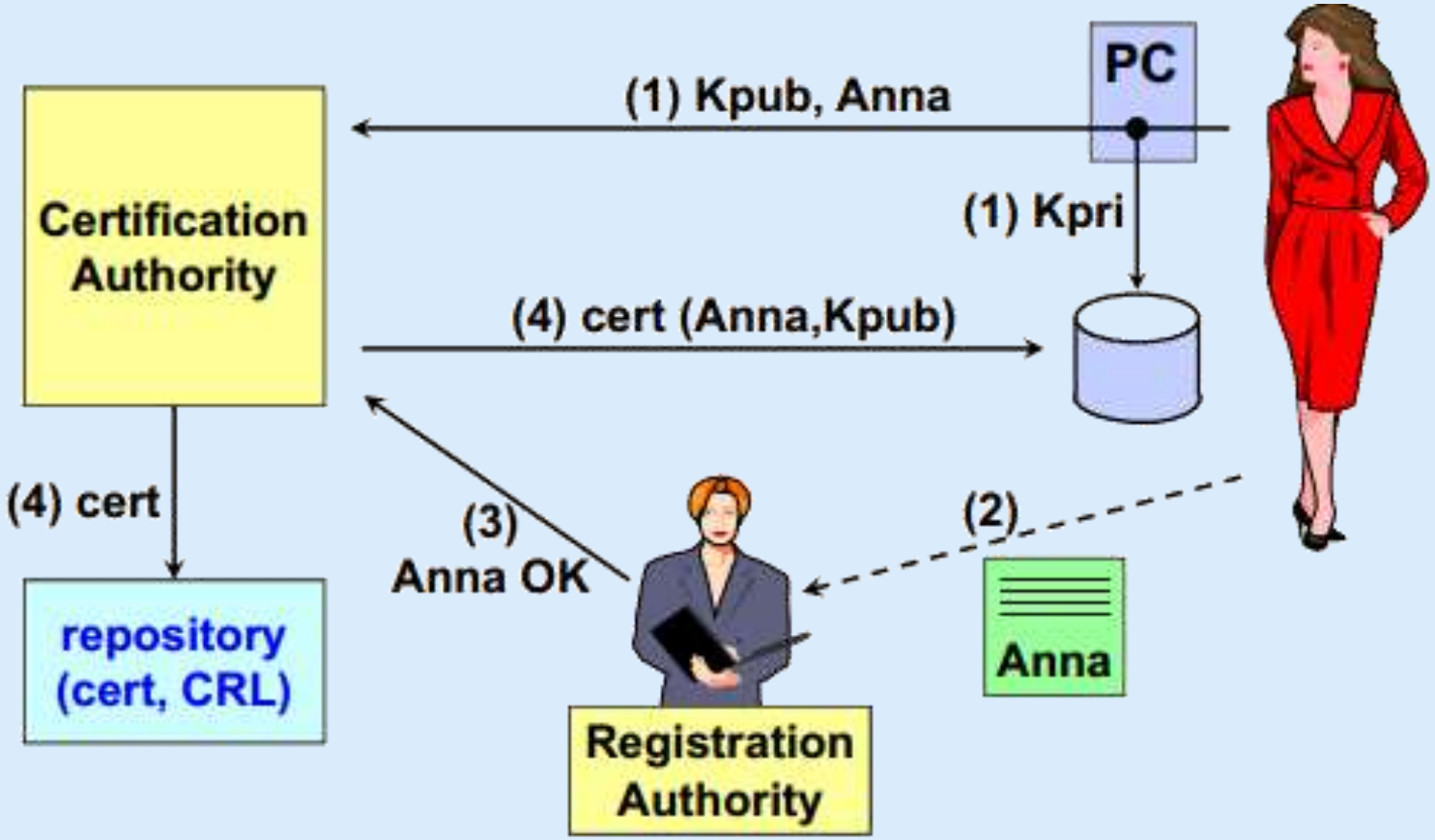
- X.509 Certificates
- Certificate Authorities (CA)
- Registration Authorities (RA)
- Public/Private Key Pairs
- Certificate Revocation Lists

Certificate Authority

- A trusted third party. Must be a secure server
  - Signs and publishes X.509 Identity certificates
  - Revokes certificates and publishes a Certification Revocation List (CRL)

- Many vendors
  - IdenTrust
  - DigiCert
  - Sectigo (Comodo)
  - Lets Encrypt: issues free certificates
  - OpenSSL: free and open source. Can be used to setup your own CA server

Certificate Issuance Process



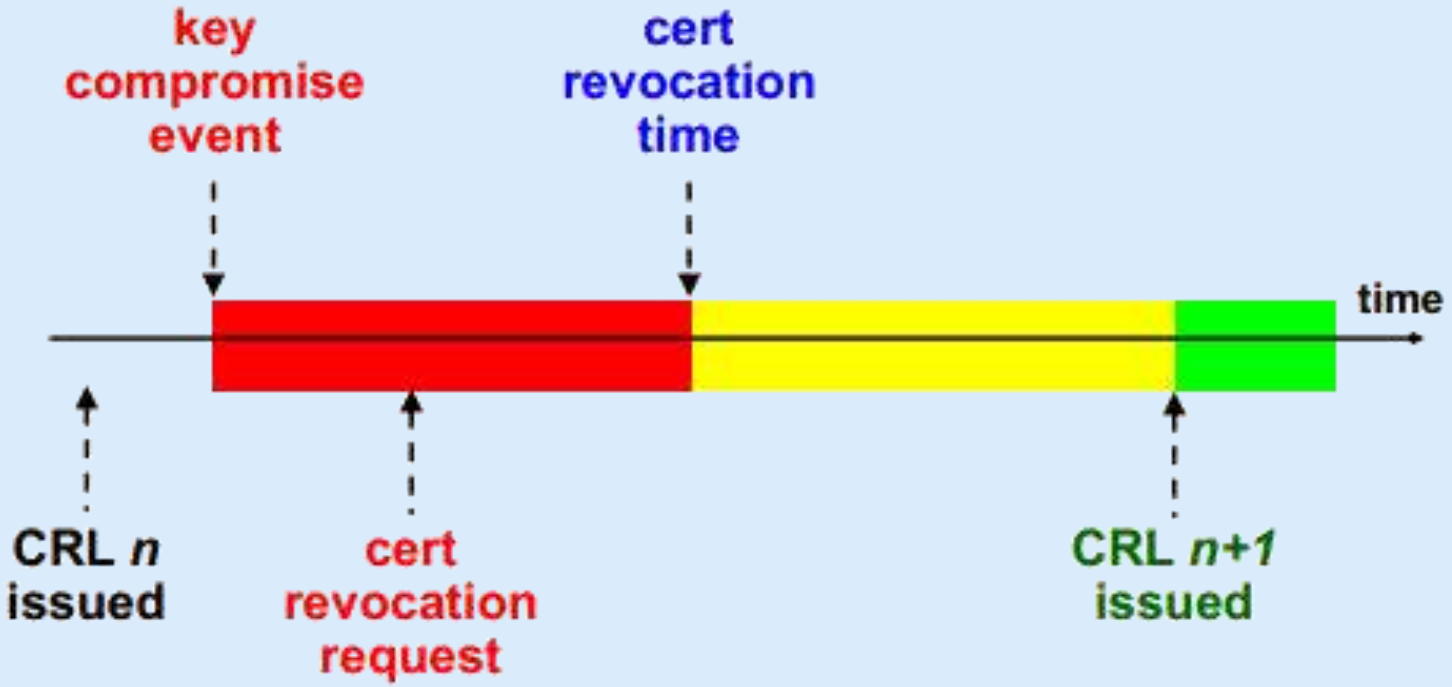
Registration Authority

- An RA is responsible for accepting requests for digital certificates and authenticating the entity making the request.
- You provide RA with information and fees
- RA verifies the information before the CA issues the certificate
- RA does not sign the certificate
- Your key pair maybe created by RA or yourself

Certificate Revocation List (CRL)

- Certificates may need to be revoked (prior to expiration) for several reasons
- Subject may request revocation because
  - Subject's private key was compromised
  - HR reasons, e.g. employee left the company
  - Temporary revocation (on "hold") e.g. resource on leave
  - Subject changed names, physical address, DNS
- CA themselves decide to revoke because
  - Subject provided false information
  - CA's private key was compromised!
- CAs maintain lists of revoked/cancelled certificates
- List published by CA frequently

Certificate Revocation Timeline



CRL Drawbacks

- Certificate revocation lists
  - Too much work on the client
  - Too much traffic on internet
    - Not used
- Alternate: Online Certificate Status Protocol
  - CA's always-online revocation server
  - Provides current information
  - Saves traffic on the internet

OCSP

- Online certificate status protocol
- IETF-PKIX standard to verify online if a certificate is valid:
  - good/verified
  - revoked
    - revocation time
    - revocation reason
  - unknown
- response must be signed by the responder server (not by the CA!)
  - the OCSP server certificate cannot be verified with OCSP itself!

OCSP Usage

subject server
e.g. youtube.com

a. request certificate
for public key A

b. issue cert-A

CA server

OCSP
responder

end user

Ahead of time

At communication time

OCSP Usage

subject server
e.g. youtube.com

a. request certificate
for public key A

b. issue cert-A

CA server

1. request
certified
public key

2. here is
cert-A

end user

OCSP
responder

Ahead of time

At communication time

OCSP Usage

subject server
e.g. youtube.com

a. request certificate
for public key A

b. issue cert-A

CA server

1. request
certified
public key

2. here is
cert-A

end user

3. ✓ not expired
and signed by a
trusted CA

OCSP
responder

Ahead of time

At communication time

OCSP Usage

subject server
e.g. youtube.com

a. request certificate
for public key A

b. issue cert-A

CA server

1. request
certified
public key

2. here is
cert-A

4. check revocation
of cert-A

5. cert-A revoked
two days ago

end user

OCSP
responder

3. ✓ not expired
and signed by a
trusted CA

Ahead of time

At communication time

OCSP Usage

subject server
e.g. youtube.com

a. request certificate
for public key A

b. issue cert-A

CA server

d. issue
cert-X

c. request cert
for public key X

1. request
certified
public key

2. here is
cert-A

4. check revocation
of cert-A

OCSP
responder

end user

5. cert-A revoked
two days ago

Must be a
signed
response

3. ✓ not expired
and signed by a
trusted CA

Ahead of time

At communication time