Public Key Management

CSS 322 – Security and Cryptography

Distributing Public Keys

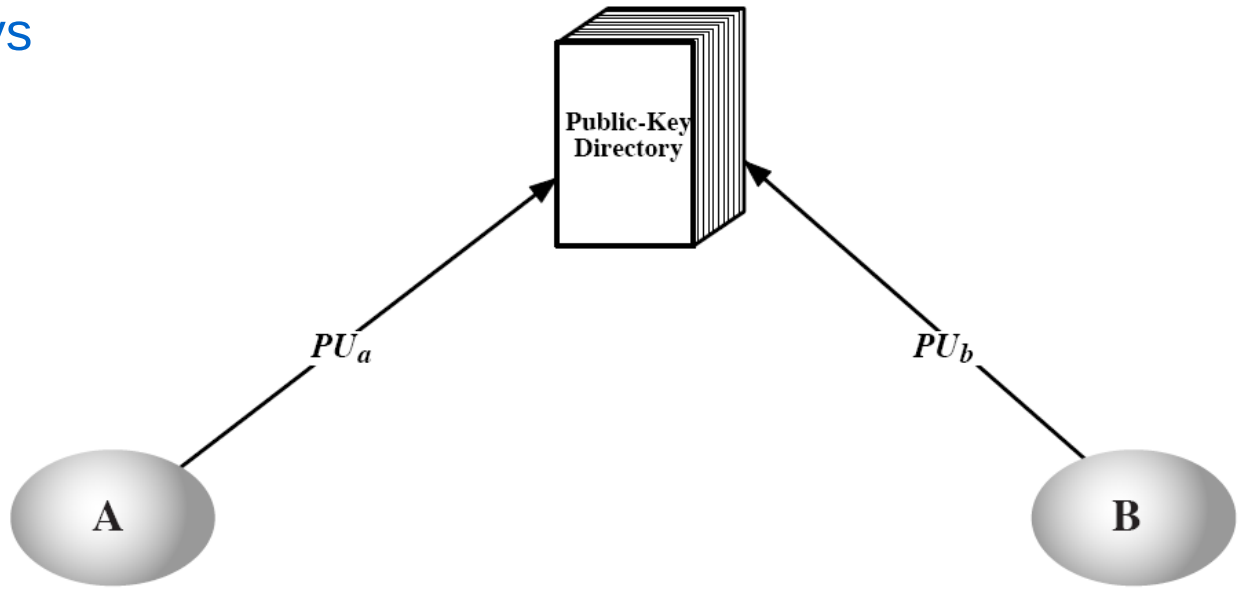
- A major advantage of public key cryptosystems (versus symmetric key) is the key distribution
  - Relatively easy to distribute keys
  - Can use public key system to distribute secret (symmetric) keys
- How to distribute public keys:
  1. Public announcements
  2. Publicly available directory
  3. Public-key authority
  4. Public-key certificate

Public Announcements

- Make your public key available in open forum:
  - Announce it at a conference
  - Publish in the newspaper
  - Include in email signature
  - Put it on your web page
  - …
- Very convenient and simple
- Major weakness:
  - The announcement can be forged
    - Anyone in this class could send an email to maillist saying “I am Steve and my public key is X”
    - Until I detect this, you can encrypt all messages intended to me

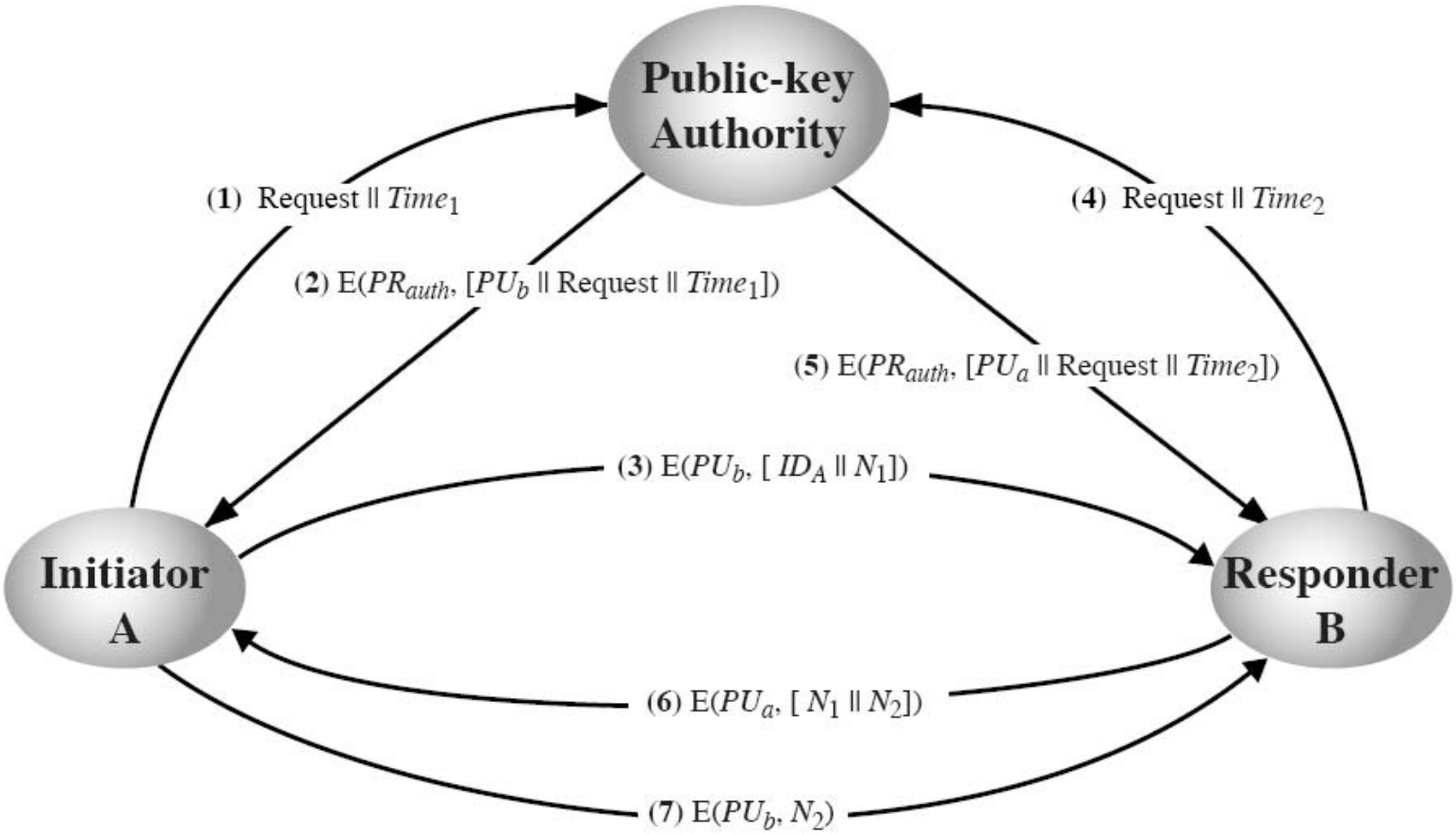
Publicly Available Directory

- All users publish their public keys to a central directory
  - Users must identify themselves before publishing
  - Users may replace public keys at any time
  - Users electronically obtain keys from directory (needs to be secure)
- More secure than public announcements, but:
  - If directory is compromised, easy for attacker to send fake public keys



Public Key Authority

- Assume:
  - Directory (central authority) maintains public keys
  - Users have public key of central authority

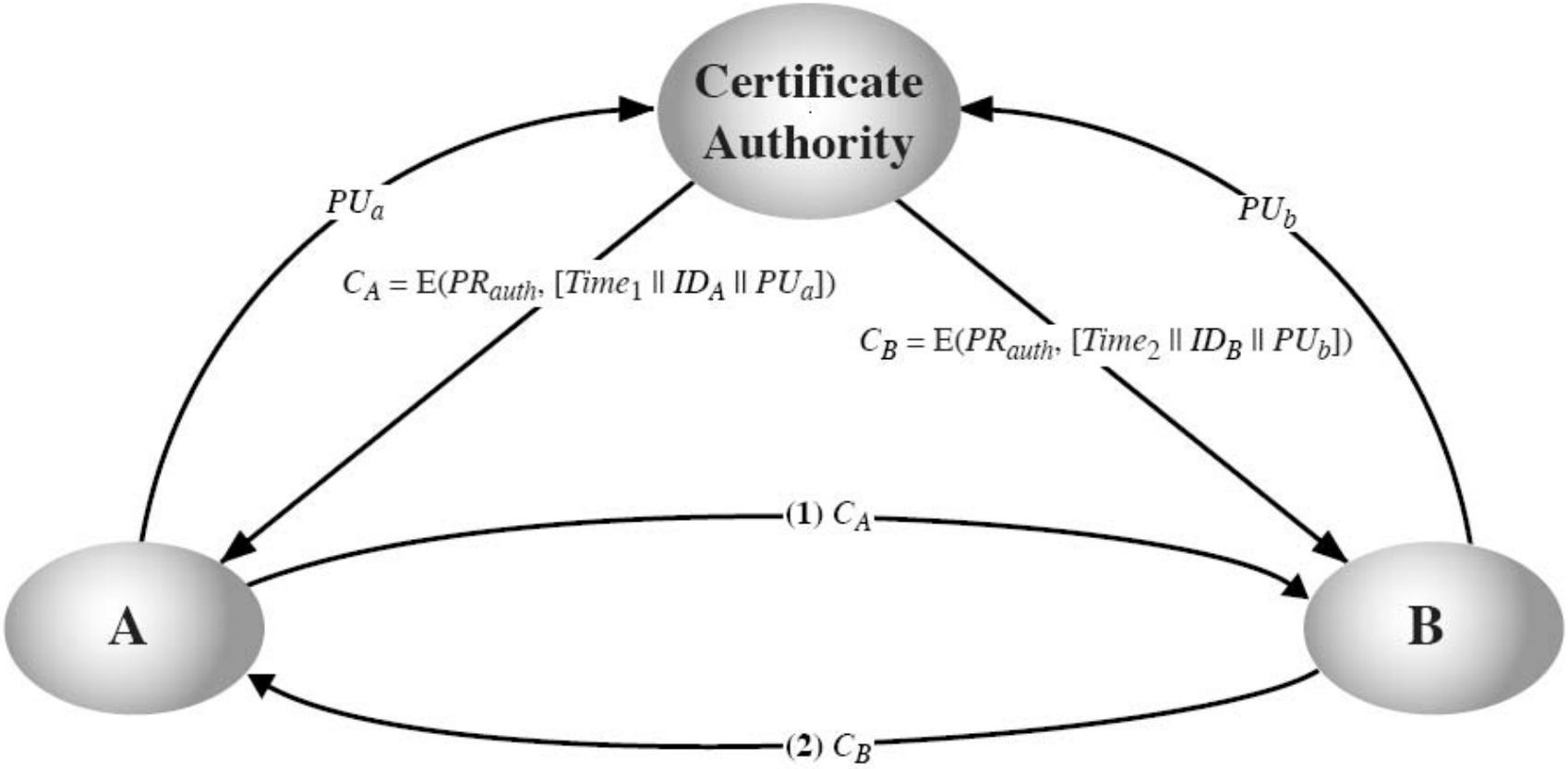


Public Key Authority

- If the users cache keys, then the first 4 steps are infrequent – only need last 3 steps to do regular updates
- Limitations:
  - Directory may become a bottleneck
    - All users must go to directory for every other user they want to contact
  - If directory is compromised, fake public keys can be issued

Public Key Certificate

- Third party is certificate authority
  - Users provide Public key to CA and receive certificate
    - This must be done in person or via secure channel



Public Key Certificate

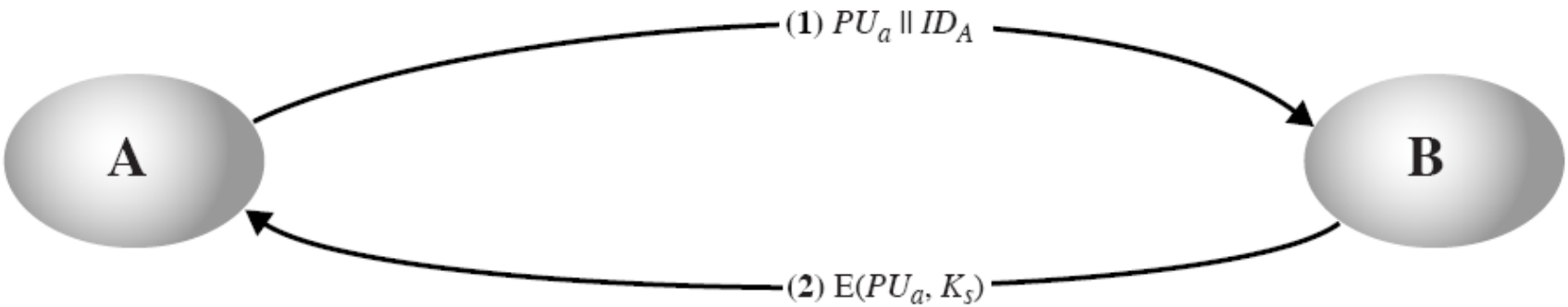
- Certificate is encrypted with CAs Private Key and contains:
  - ID of user
  - Public key of user
  - Time of issue
- If private key is compromised, obtain new certificate and inform all parties of new certificate
- X.509 is a standard for public key certificates:
  - Used in IPsec, SSL and other applications

Distributing Secret Keys

- Public key encryption is significantly slower than symmetric key encryption
- In practice, use public key encryption to create secure channel, then exchange symmetric/private keys for data encryption

Simple Secret Key Distribution

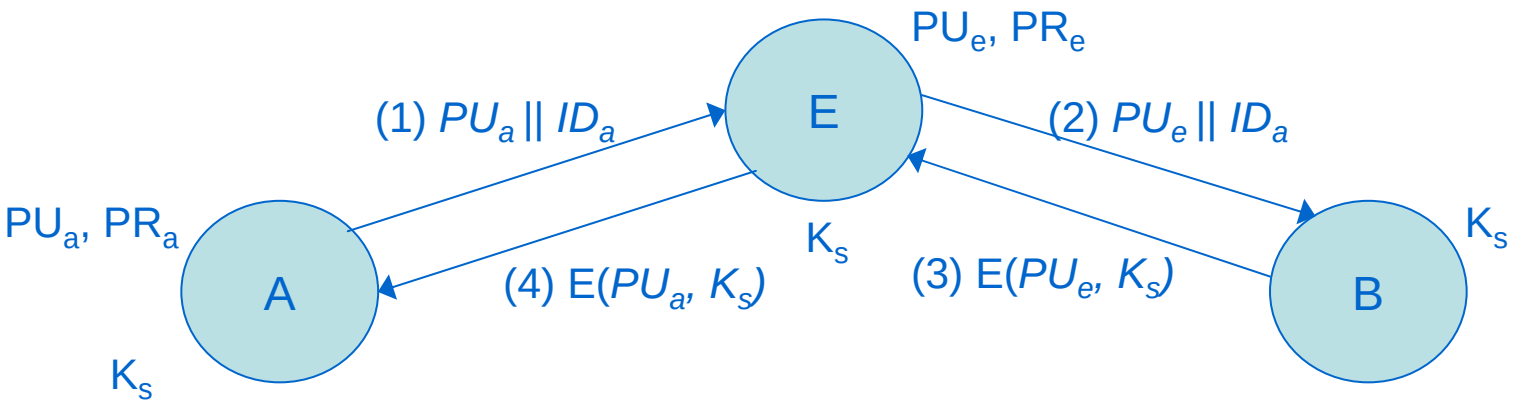
- Steps:
  - A generates own public/private key and sends Public key to B
  - B generates secret key and sends it back to A, encrypted with A's public key
  - Now both A and B have secret key and can discard public/private keys



  - Simple scheme, which creates secure connection

Man-in-the-Middle Attack

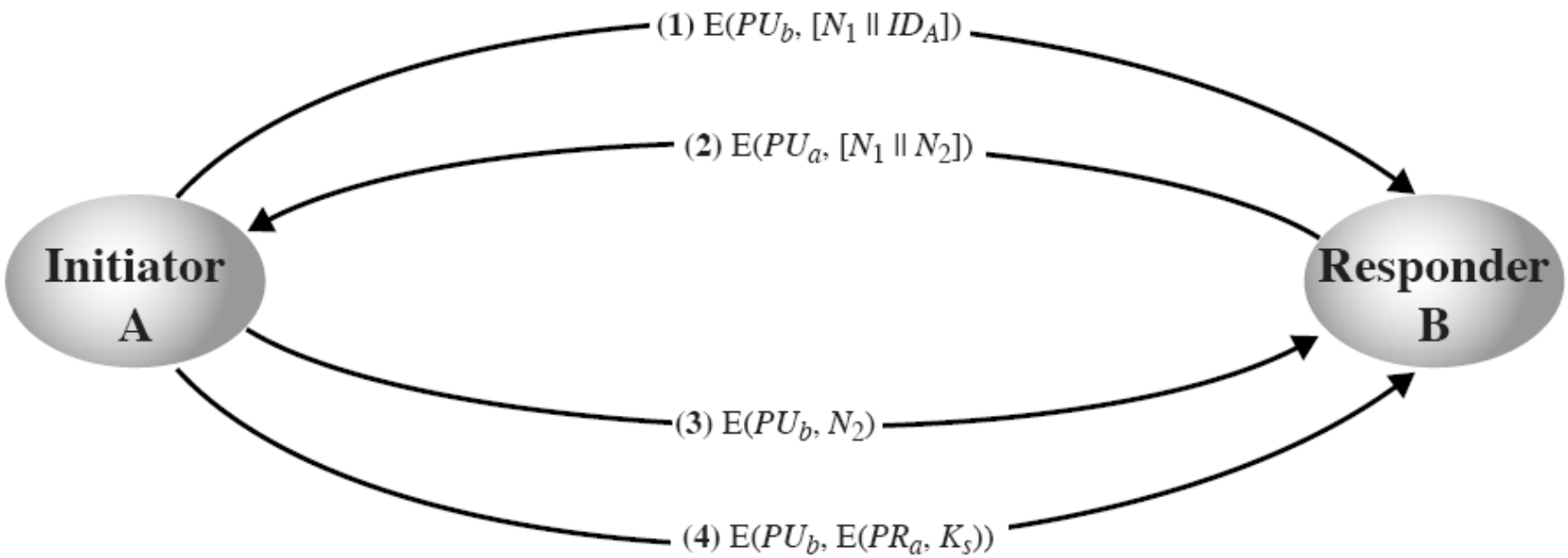
- The simple scheme can be attacked by a third party C:



- Now A and B have K_s and can send encrypted data
  - But C also has K_s and can decrypt all the data
  - A or B do not know C has secret key

Secret Key Distribution

- With Confidentiality and Authentication
- Assume A and B have exchanged public keys (e.g. using certificates)



Diffie-Hellman Exchange

- Diffie and Hellman proposed public key cryptosystems in 1976
  - They described a method for exchanging keys
  - Based on discrete logarithms
    - Easy to calculate exponentials module a prime
    - Hard to calculate inverse: discrete logarithms

      `Given integer b, prime p, primitive root a of p:`

      $$b \equiv a^i \pmod{p}$$

      $$i = discretelog_{a,p}(b)$$
  - Only used for exchange of secret value

Diffie-Hellman Steps

Global Public Elements

q	prime number
α	$\alpha < q$ and α a primitive root of q

User A Key Generation

Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{X_A} \bmod q$

User B Key Generation

Select private X_B	$X_B < q$
Calculate public Y_B	$Y_B = \alpha^{X_B} \bmod q$

Calculation of Secret Key by User A

$K = (Y_B)^{X_A} \bmod q$

Calculation of Secret Key by User B

$K = (Y_A)^{X_B} \bmod q$