SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

Course Code and Name : 19IT602– CRYPTOGRAPHY AND CYBER SECURITY

III YEAR / VI SEMESTER

Unit 3: ASYMMETRIC KEY CRYPTOGRAPHY

Topic : RSA cryptosystem

RSA

- by Rivest, Shamir & Adleman of MIT in 1977
- best known & widely used public-key scheme
- to encrypt a message M the sender:
  - obtains **public key** of recipient **PU={e,n}**
  - computes: **$C = M^e \bmod n$, where $0 \le M < n$**
- to decrypt the ciphertext C the owner:
  - uses their **private key PR={d,n}**
  - computes: **$M = C^d \bmod n$**

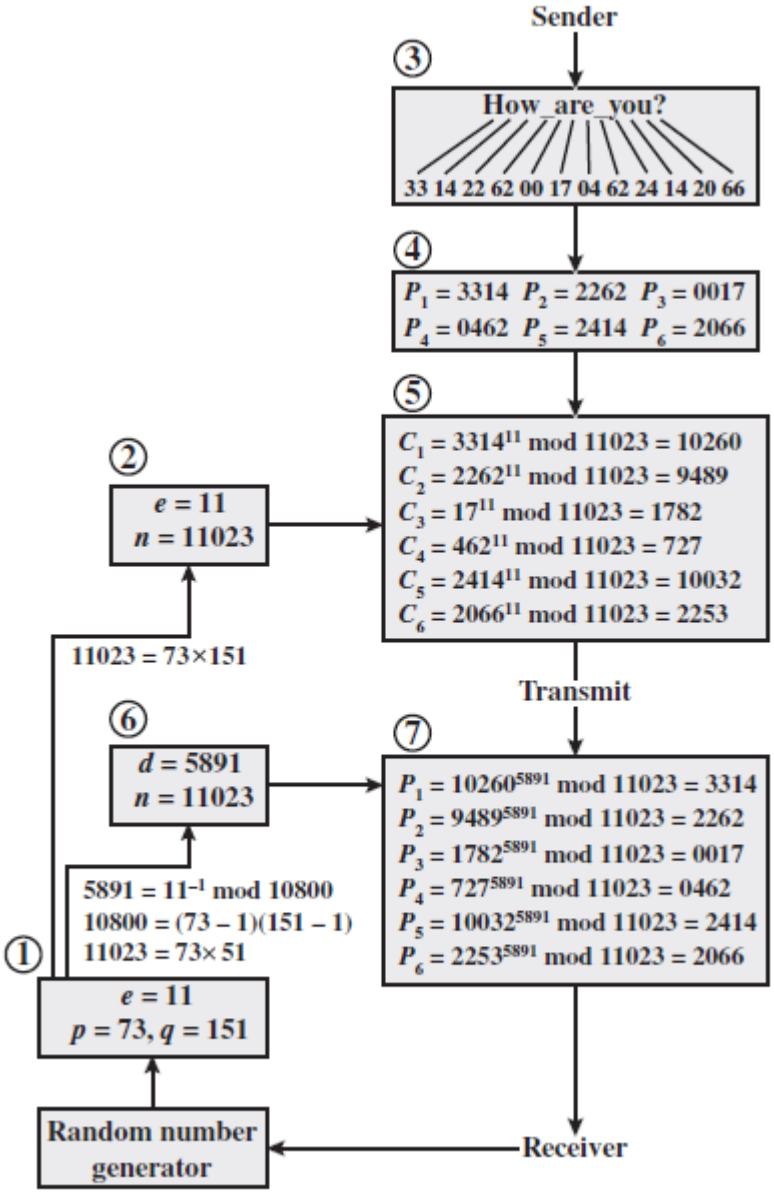
RSA

- **Key Generation by Alice**
  - Select p, q — p and q both prime, p q
  - Calculate n — n= p * q
  - Calculate ϕ(n) — ϕ(n) = (p - 1)(q - 1)
  - Select integer e — gcd (ϕ(n),e) = 1; 1 < e < ϕ(n)
  - Calculate d — d ≡ e-1 (mod ϕ(n))
  - Public key — PU = {e, n}
  - Private key — PR = {d, n}

RSA

- **Encryption by Bob with Alice's Public Key**
  - Plaintext: $M < n$
  - Ciphertext: $C = M^e \bmod n$
- **Decryption by Alice with Alice's Public Key**
  - Ciphertext: C
  - Plaintext: $M = C^d \bmod n$

RSA Example


Sender
3
How_are_you?
33 14 22 62 00 17 04 62 24 14 20 66
4
$P_1 = 3314$ $P_2 = 2262$ $P_3 = 0017$
$P_4 = 0462$ $P_5 = 2414$ $P_6 = 2066$
5
$C_1 = 3314^{11} \bmod 11023 = 10260$
$C_2 = 2262^{11} \bmod 11023 = 9489$
$C_3 = 17^{11} \bmod 11023 = 1782$
$C_4 = 462^{11} \bmod 11023 = 727$
$C_5 = 2414^{11} \bmod 11023 = 10032$
$C_6 = 2066^{11} \bmod 11023 = 2253$
2
$e = 11$
$n = 11023$
11023 = 73×151
Transmit
6
$d = 5891$
$n = 11023$
7
$P_1 = 10260^{5891} \bmod 11023 = 3314$
$P_2 = 9489^{5891} \bmod 11023 = 2262$
$P_3 = 1782^{5891} \bmod 11023 = 0017$
$P_4 = 727^{5891} \bmod 11023 = 0462$
$P_5 = 10032^{5891} \bmod 11023 = 2414$
$P_6 = 2253^{5891} \bmod 11023 = 2066$
$5891 = 11^{-1} \bmod 10800$
$10800 = (73 - 1)(151 - 1)$
$11023 = 73 \times 51$
1
$e = 11$
$p = 73, q = 151$
Random number generator
Receiver

RSA Security

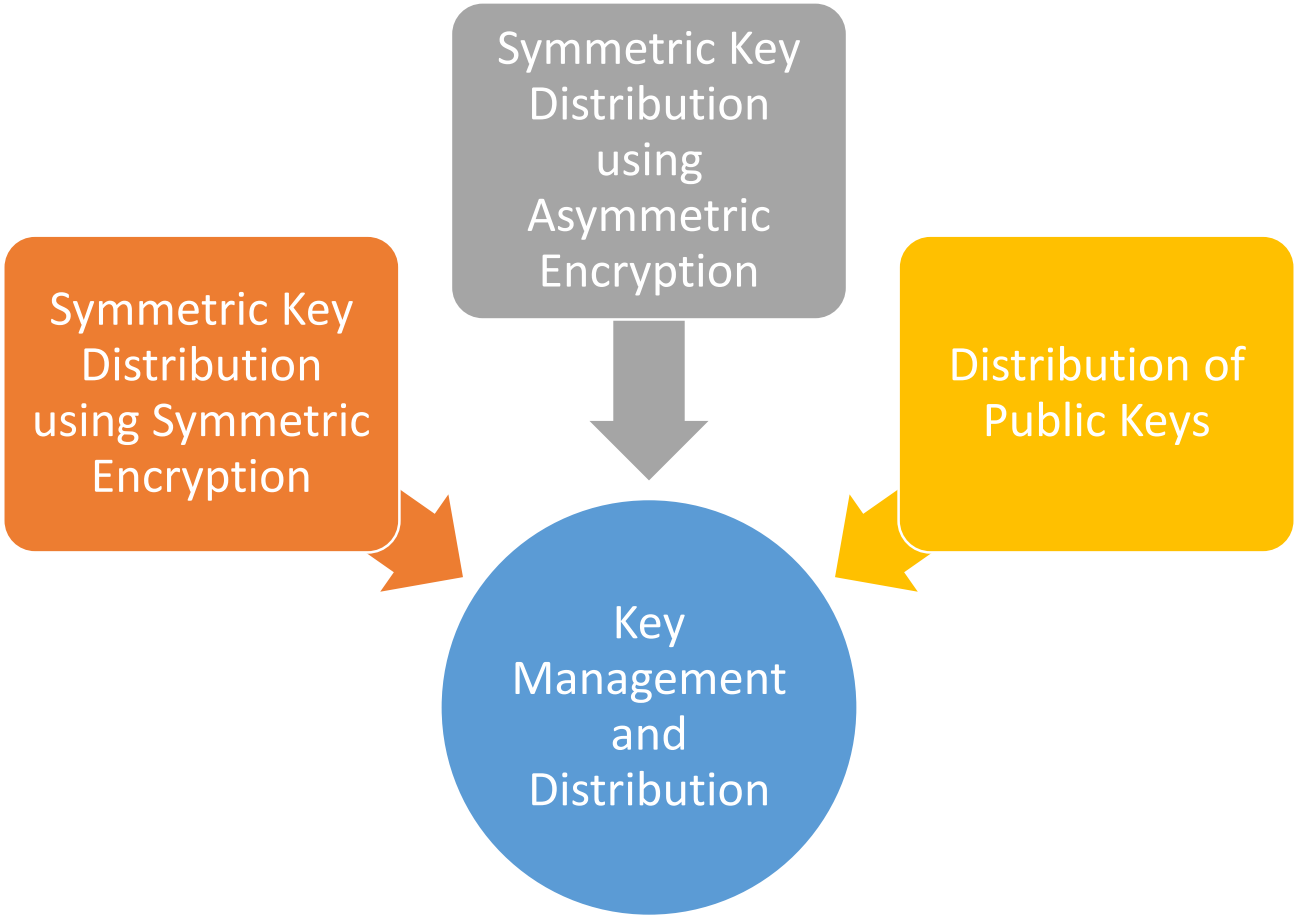
- possible approaches to attacking RSA are:
  - brute force key search - infeasible given size of numbers
  - mathematical attacks - based on difficulty of computing ø(n), by factoring modulus n
  - timing attacks - on running of decryption
  - chosen ciphertext attacks - given properties of RSA

Key Management

Key Management and Distribution

- Key management is the set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties.
- Key Distribution is the function that delivers a key to two parties who wish to exchange secure encrypted data.

Key Management and Distribution



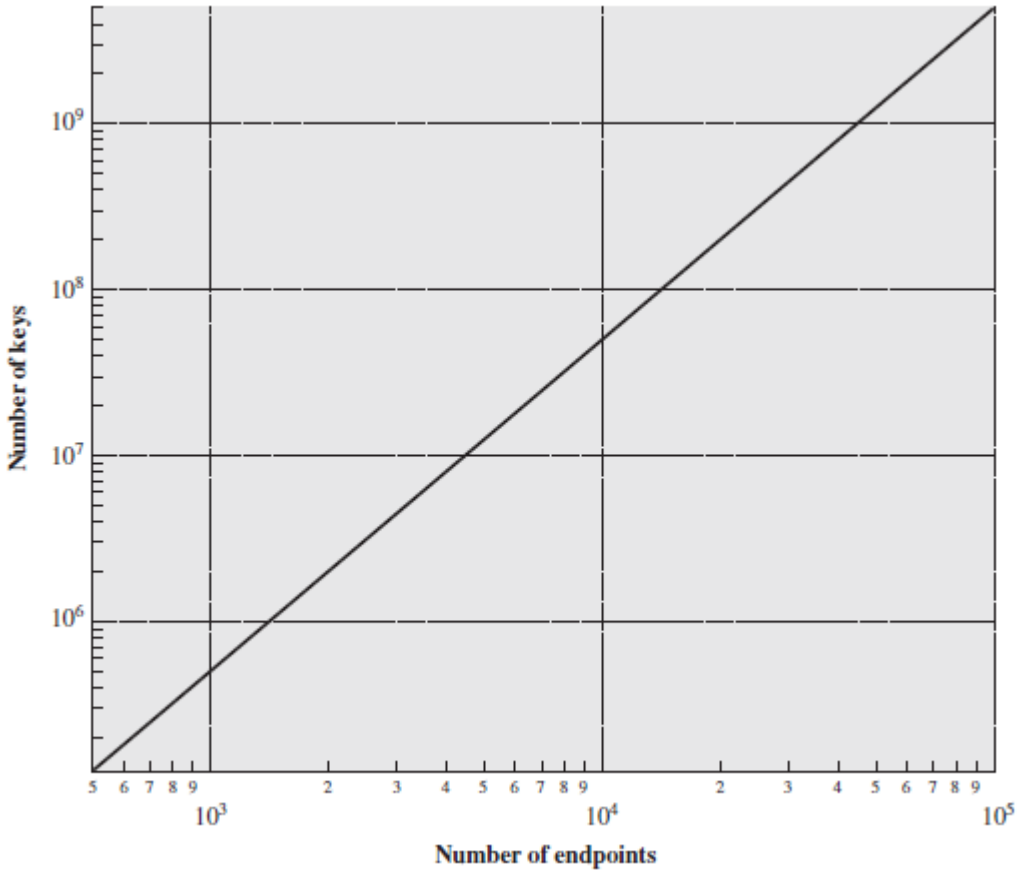
Symmetric Key Distribution using Symmetric Encryption

- Symmetric schemes require both parties to share a common secret key
- Issue is how to securely distribute this key
- whilst protecting it from others
- Frequent key changes can be desirable
- Often secure system failure due to a break in the key distribution scheme

Alternatives / Ways of Key Distribution

- A and B are two parties
  1. A can select key and physically deliver to B
  2. third party can select & physically deliver key to A & B
  3. if A & B have communicated previously can use previous key to encrypt a new key
  4. if A & B have secure/encrypted communications with a third party C, C can relay key between A & B
- 1 & 2 – Simplest but manual delivery awkward and distributed systems makes it difficult
- 3 – suffers if the attacker gains any one key.
- 4 – Widely adopted

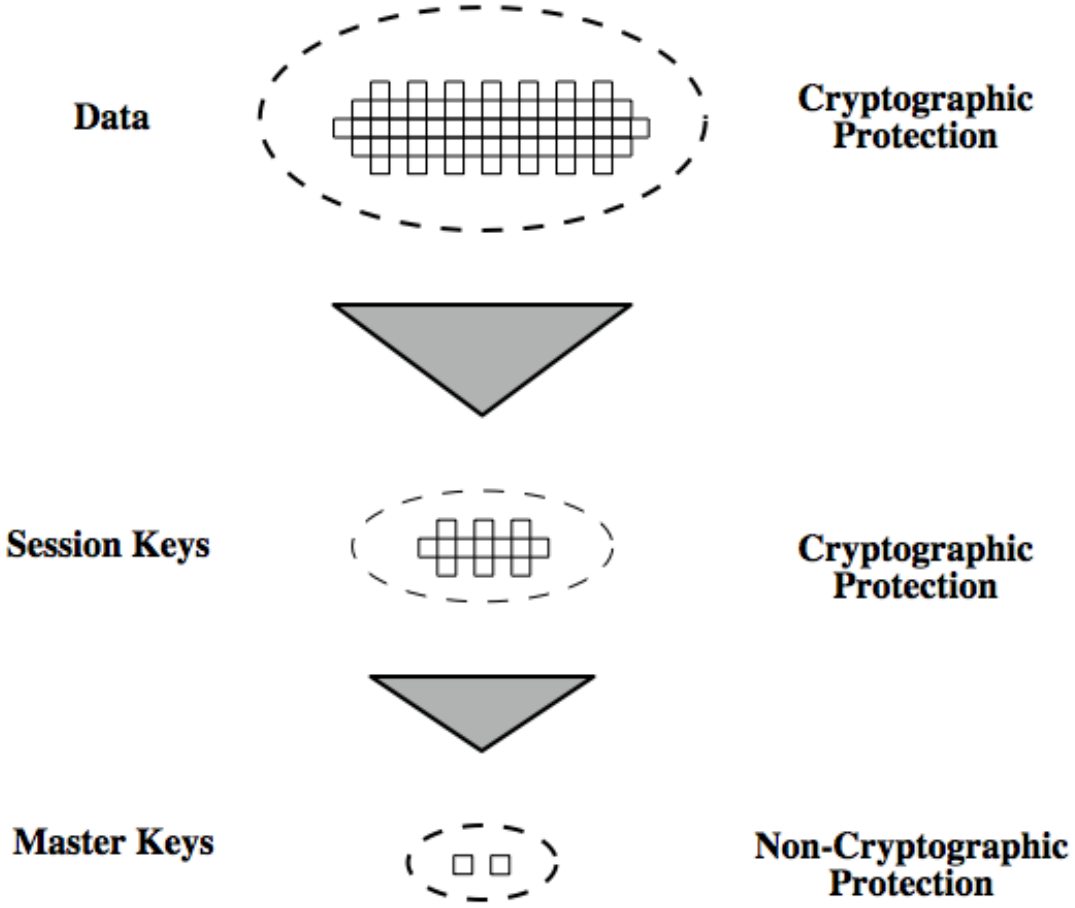
Number of Keys Required to Support Arbitrary Connections between Endpoints



Key Hierarchy

- temporary key
- used for encryption of data between users
- for one logical session then discarded

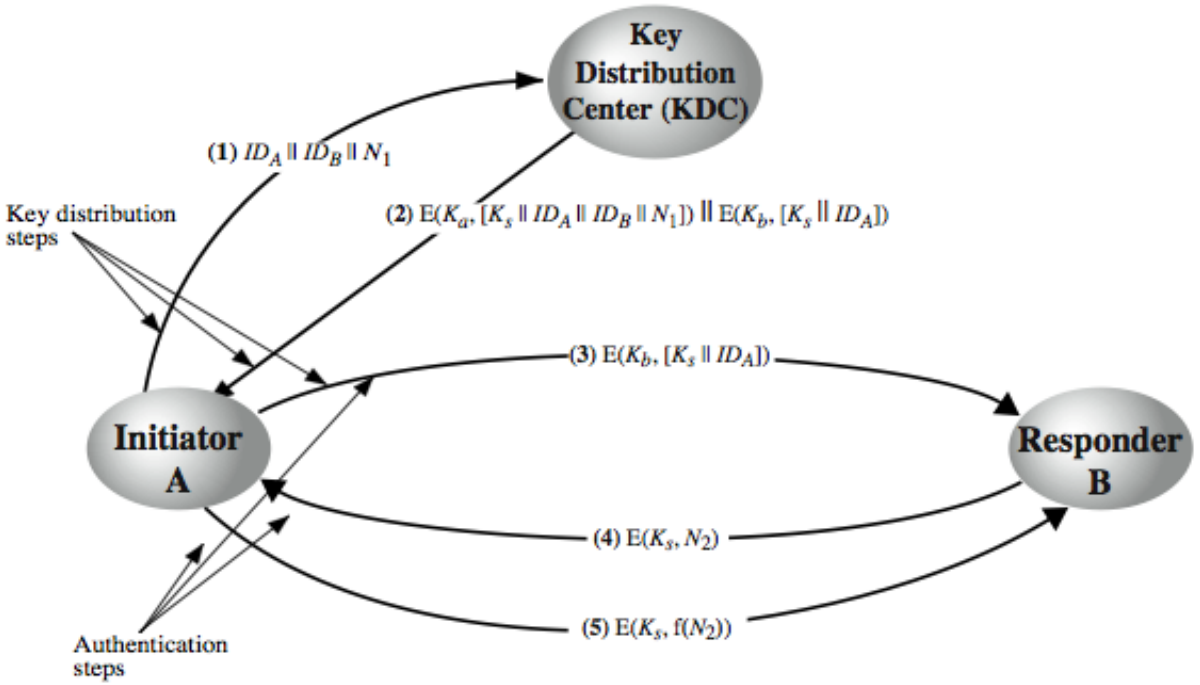
- used to encrypt session keys
- shared by user & key distribution center



Key Distribution Scenario

- K_s – Session Key
- K_a and K_b – Master Key that A and B shares with KDC
- $f(N_2)$ – Performs some transformation on N_2

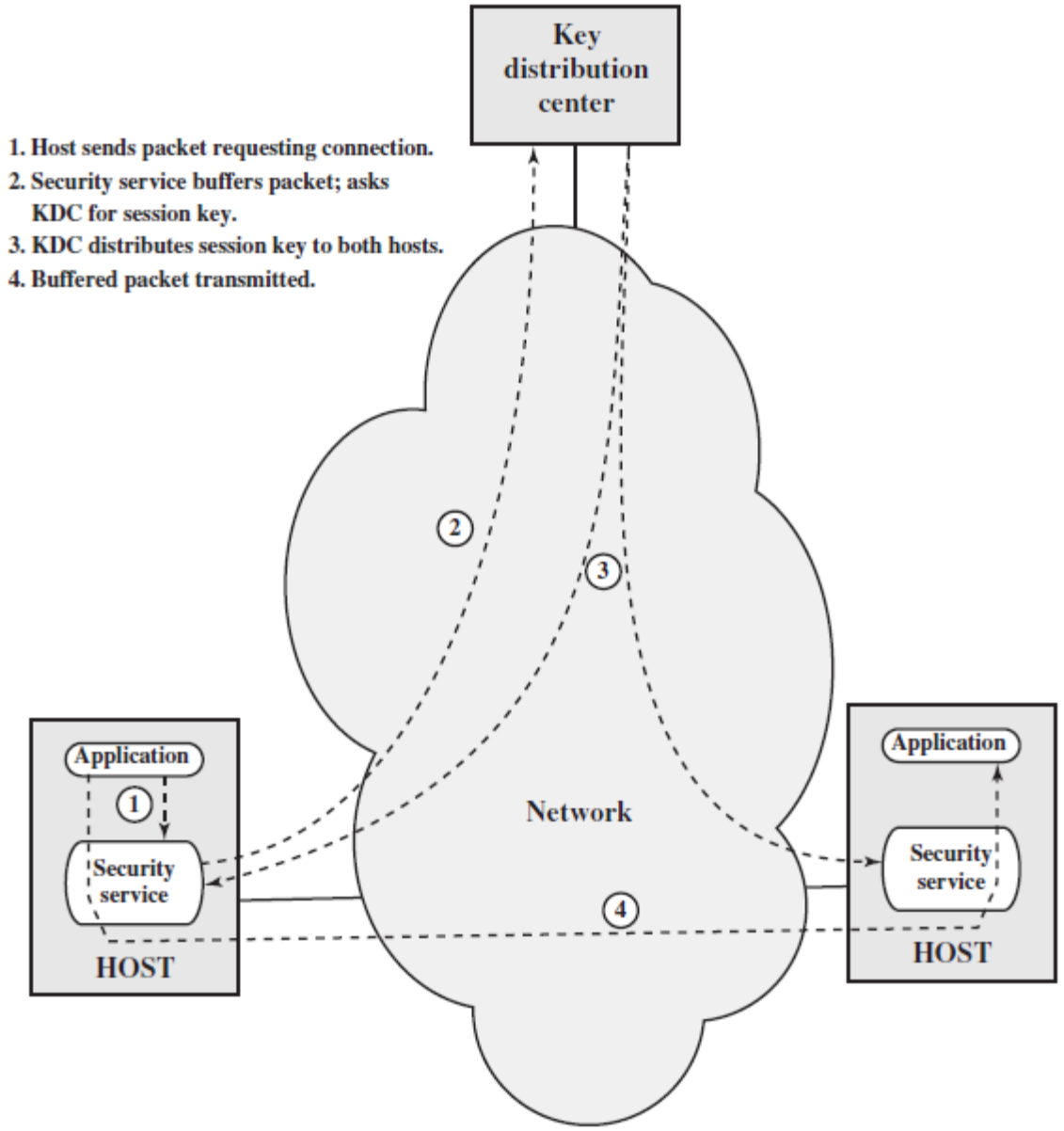
Nonce –Timestamp – counter – random number - Unique Identifier for each request



Key Distribution Issues

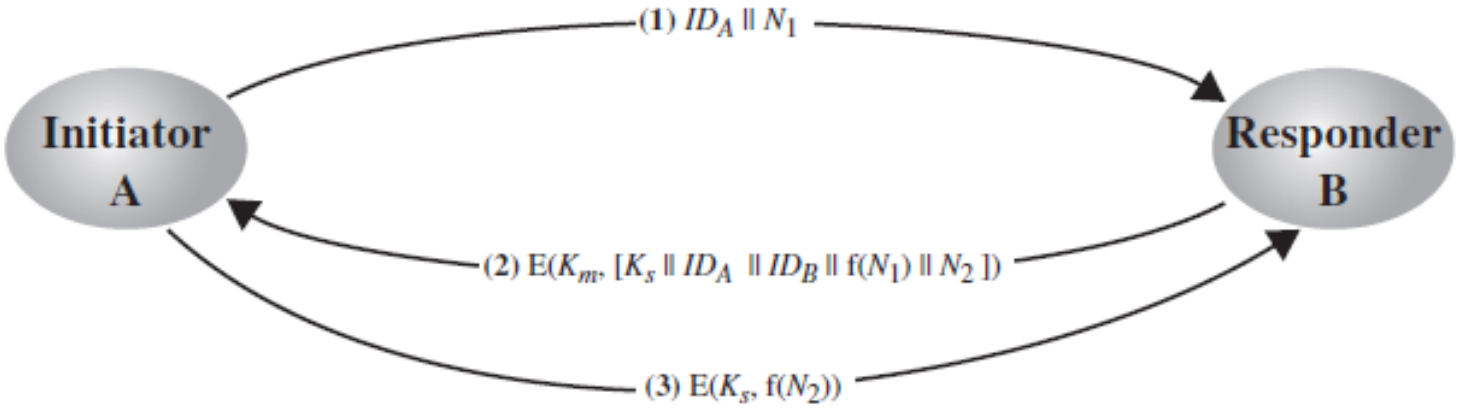
- Hierarchies of KDC's required for large networks, but must trust each other
- Session key lifetimes should be limited for greater security
- Use of automatic key distribution on behalf of users, but must trust system
- Use of decentralized key distribution
- Controlling key usage

Automated Key Distribution

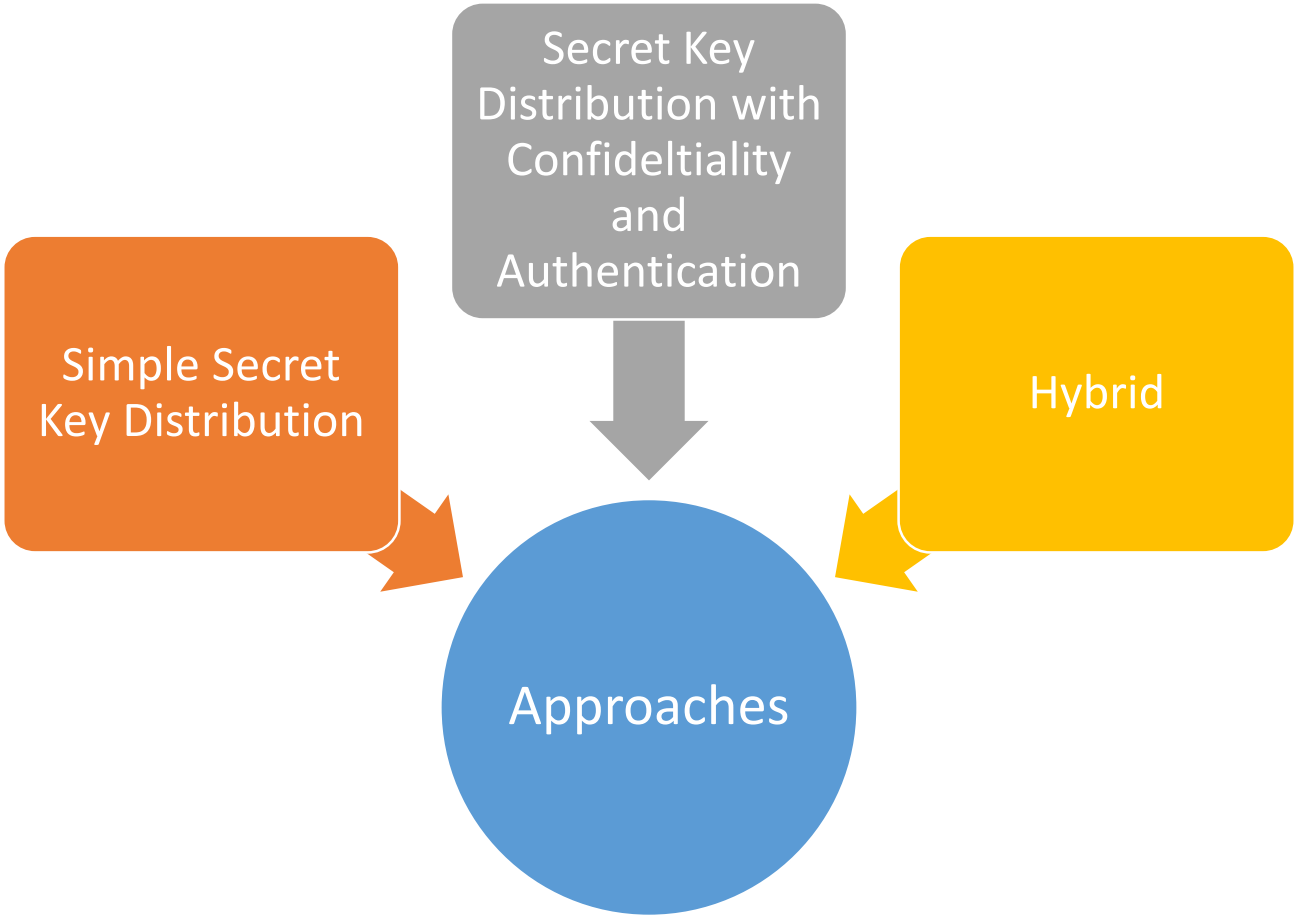


Decentralized Key Control

- Not Practical for Large Networks.
- Master Keys are short – Cryptanalysis Difficult.

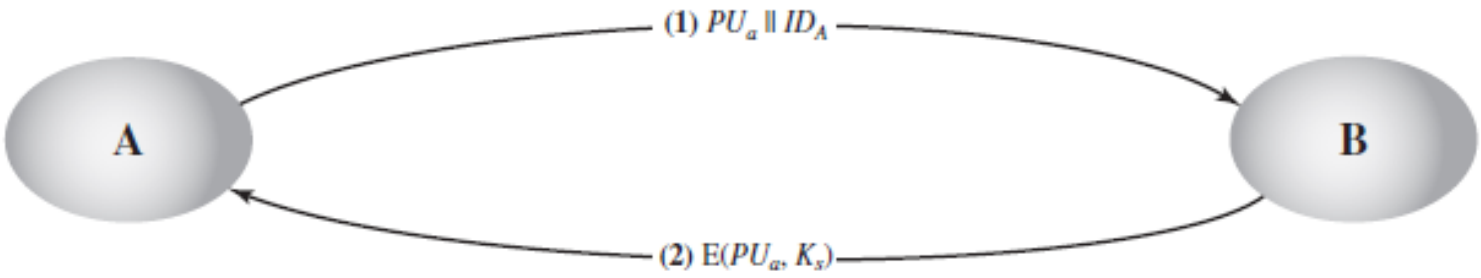


Symmetric Key Distribution using Asymmetric Encryption

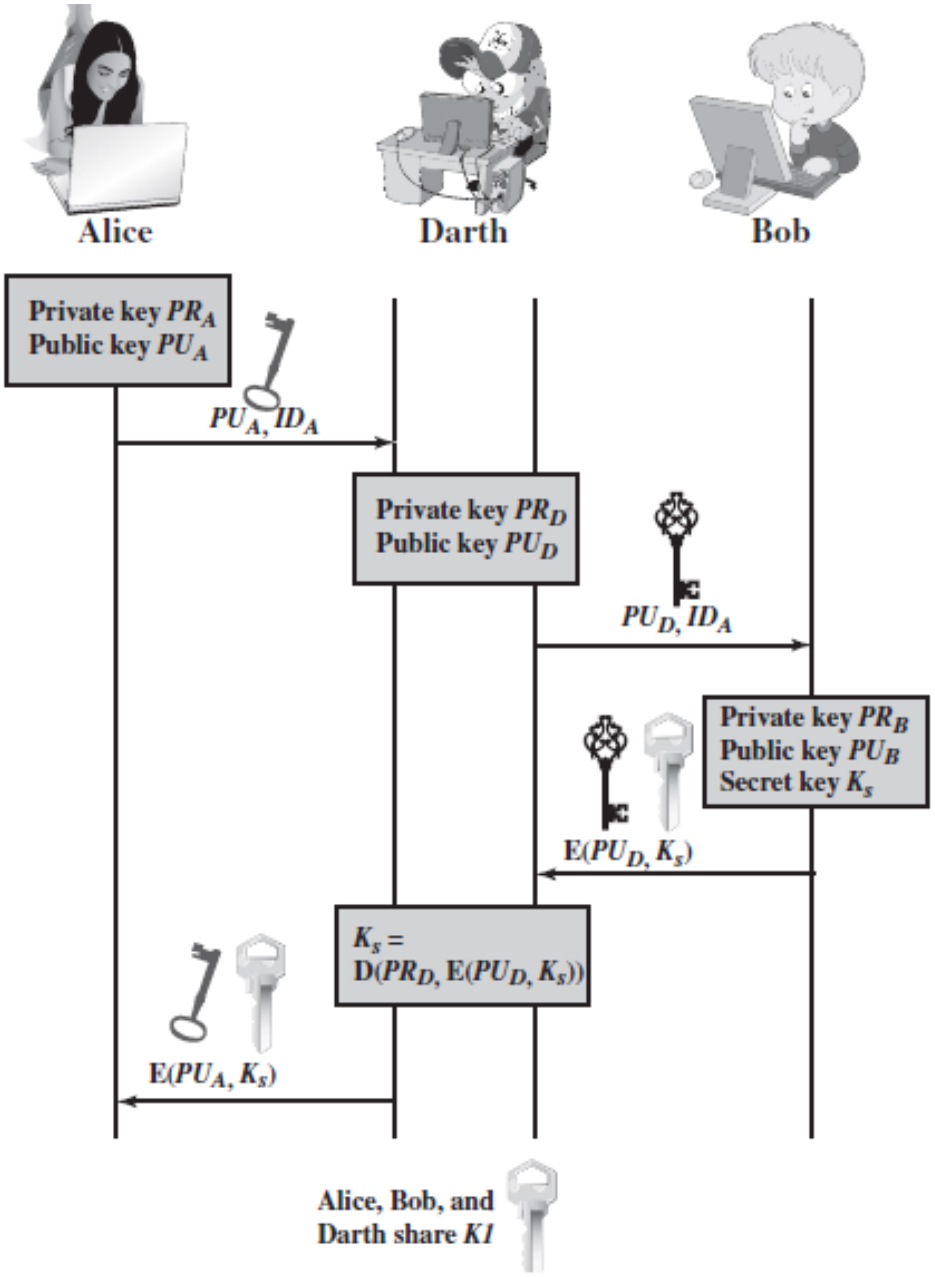


Simple Secret Key Distribution

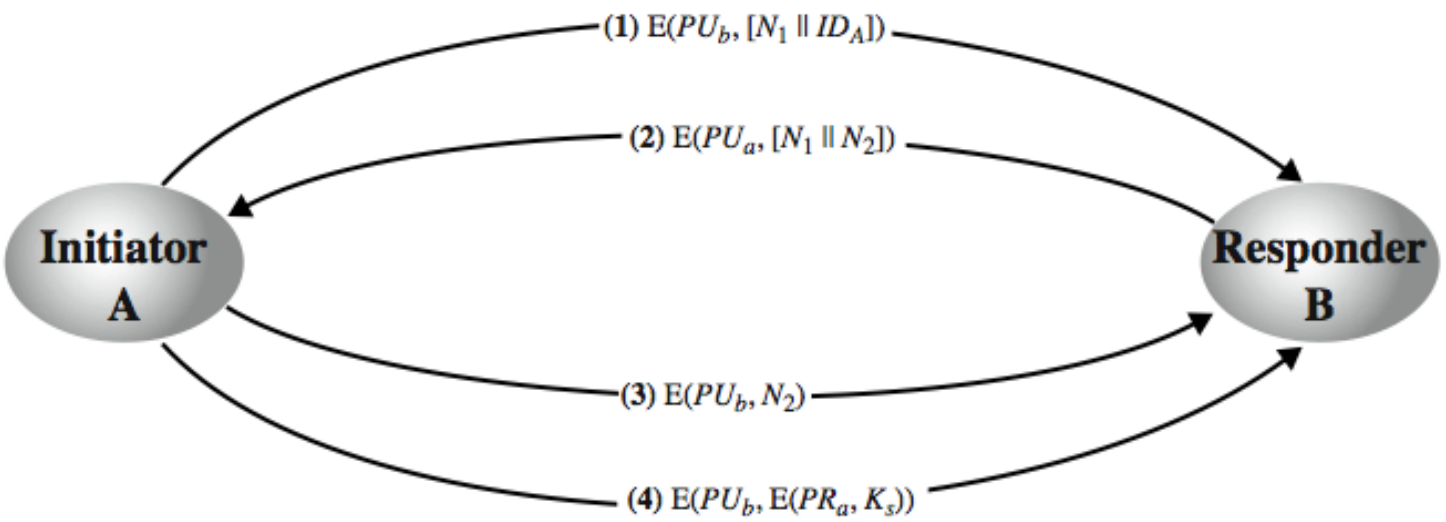
- Merkle proposed this very simple scheme
  - allows secure communications
  - no keys before/after exist



Man-in-the-Middle Attack



Secret Key Distribution with Confidentiality and Authentication



Hybrid Key Distribution

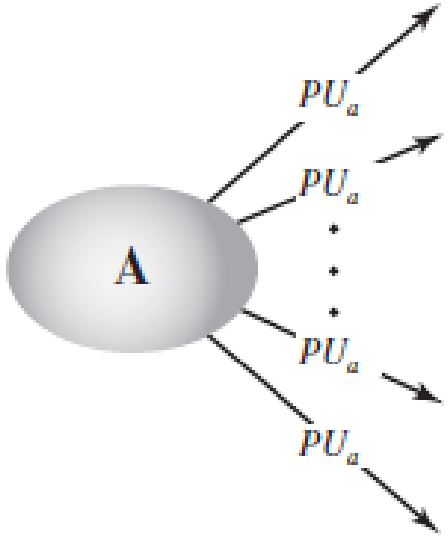
- retain use of private-key KDC
- shares secret master key with each user
- distributes session key using master key
  - public-key used to distribute master keys
- especially useful with widely distributed users
  - rationale
  - performance
  - backward compatibility

Distribution of Public Keys

- can be considered as using one of:
  - public announcement
  - publicly available directory
  - public-key authority
  - public-key certificates

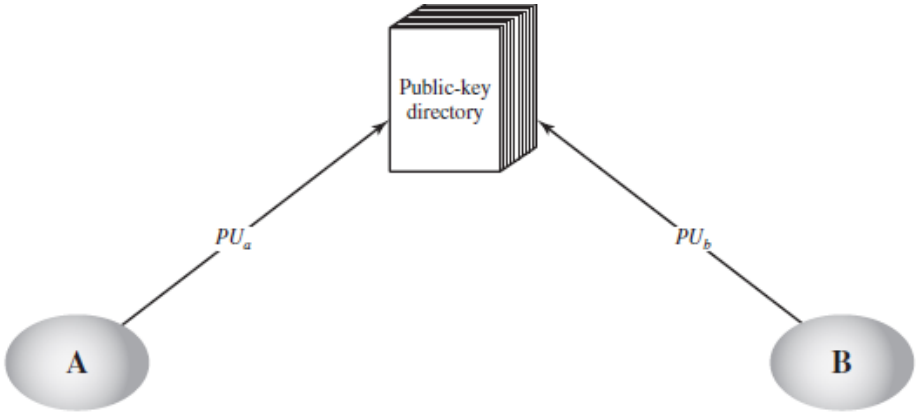
Public Announcement

- users distribute public keys to recipients or broadcast to community at large
  - Example: append PGP keys to email messages or post to news groups or email list
- major weakness is forgery
  - anyone can create a key claiming to be someone else and broadcast it
  - until forgery is discovered can masquerade as claimed user



Publicly Available Directory

- can obtain greater security by registering keys with a public directory
- still vulnerable to tampering or forgery

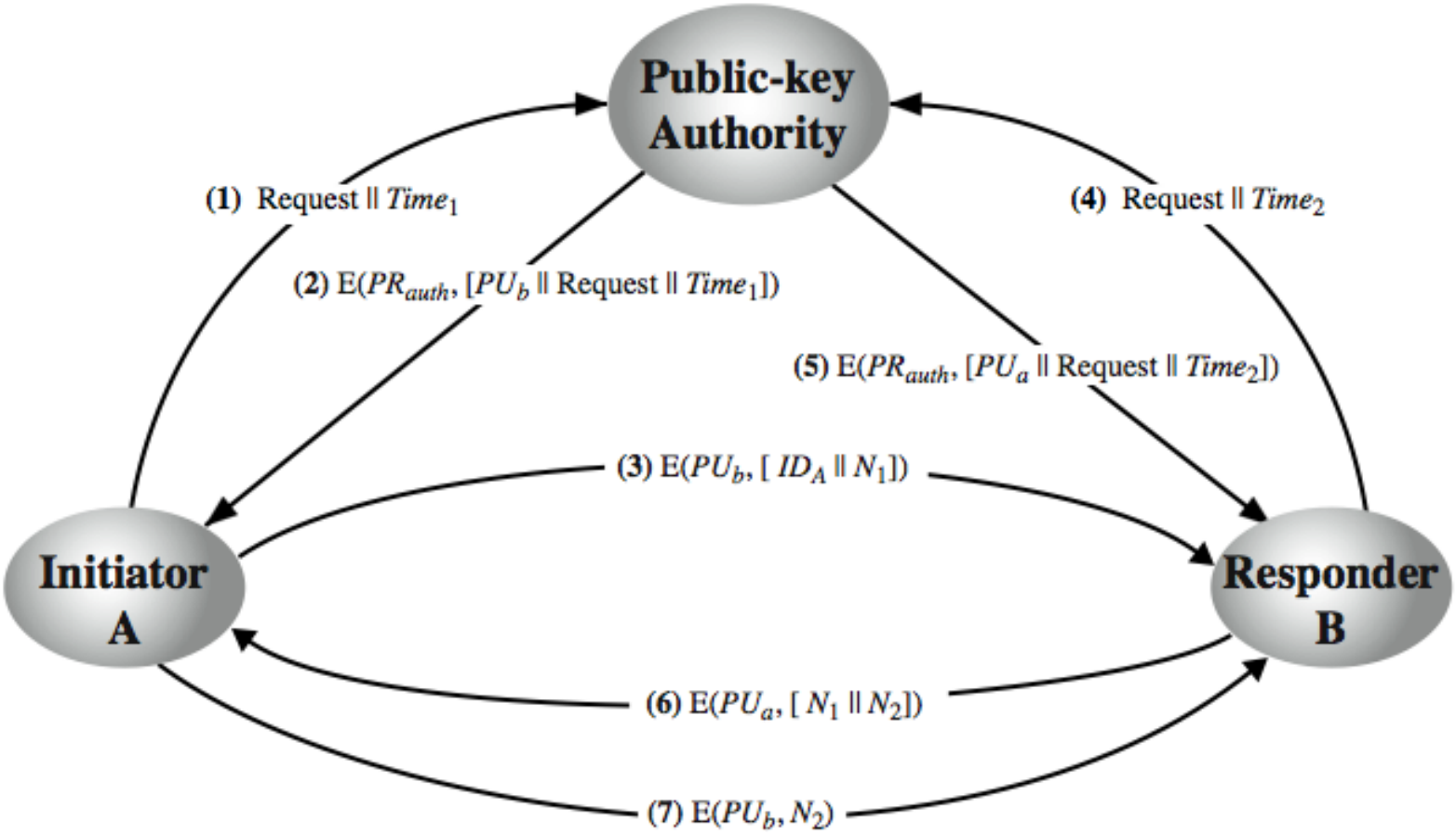


- directory must be trusted with properties:
  - contains {name,public-key} entries
  - participants register securely with directory
  - participants can replace key at any time
  - directory is periodically published
  - directory can be accessed electronically

Public-Key Authority

- improve security by tightening control over distribution of keys from directory
- has properties of directory
- and requires users to know public key for the directory
- then users interact with directory to obtain any desired public key securely
  - does require real-time access to directory when keys are needed
  - may be vulnerable to tampering

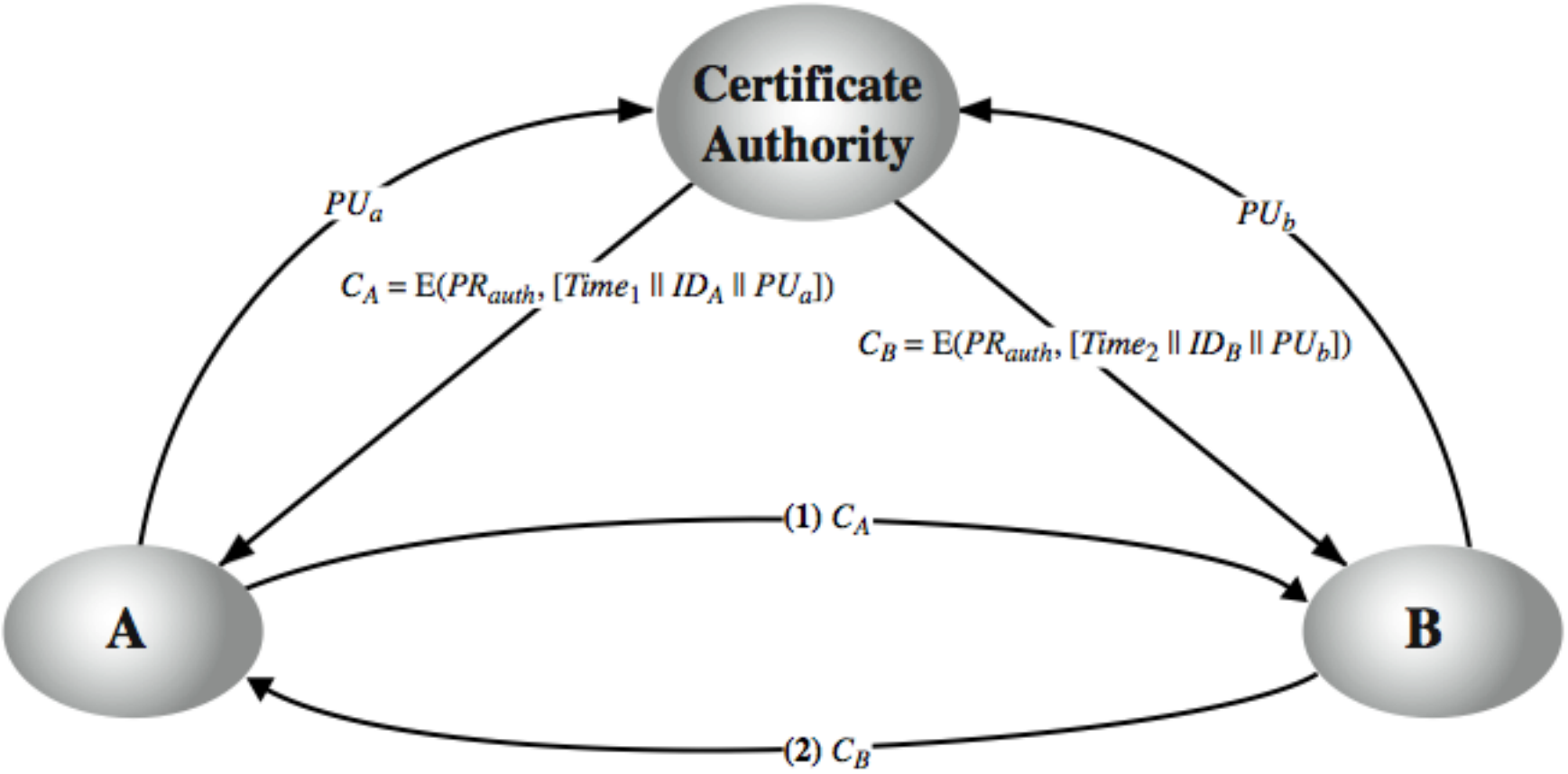
Public-Key Authority



Public-Key Certificates

- certificates allow key exchange without real-time access to public-key authority
- a certificate binds identity to public key
  - usually with other info such as period of validity, rights of use etc
- with all contents signed by a trusted Public-Key or Certificate Authority (CA)
- can be verified by anyone who knows the public-key authorities public-key

Public-Key Certificate



Thank You