CS549: Computer and Network Security

Key Distribution

Dr. Manas Khatua
Assistant Professor
Dept. of Computer Science & Engineering
Indian Institute of Technology Guwahati
URL: http://manaskhatua.github.io/
Email: manaskhatua@iitg.ac.in

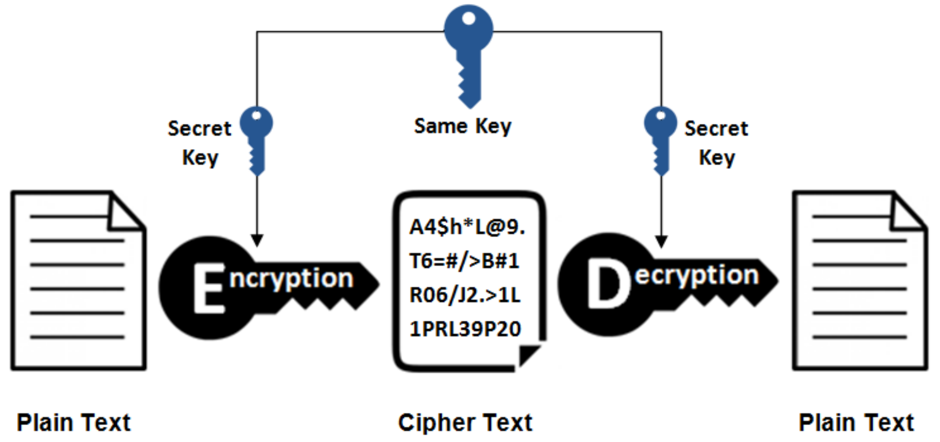
“श्रद्धावान् लभते ज्ञानं तत्परः संयतेन्द्रियः”

Content

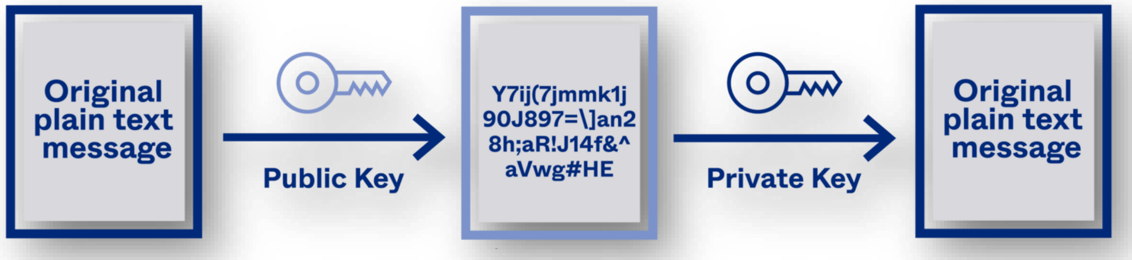
- ✓ Introduction to Key distribution
  - ✓ Challenges
  - ✓ Key distribution techniques
    - ✓ Symmetric Key Distribution
    - ✓ Asymmetric Key Distribution
- ✓ Symmetric Key distribution
  - ✓ Using Symmetric Encryption
  - ✓ Using Asymmetric Encryption
- ✓ Asymmetric Key distribution
  - ✓ Different Methods
  - ✓ PKI
  - ✓ X.509 certificate
- ✓ MITM Attack
  - ✓ on Symmetric Key Distribution using Asymmetric Encryption
  - ✓ on Diffie-Hellman Key Exchange

Key Distribution

Symmetric Key



Asymmetric Key

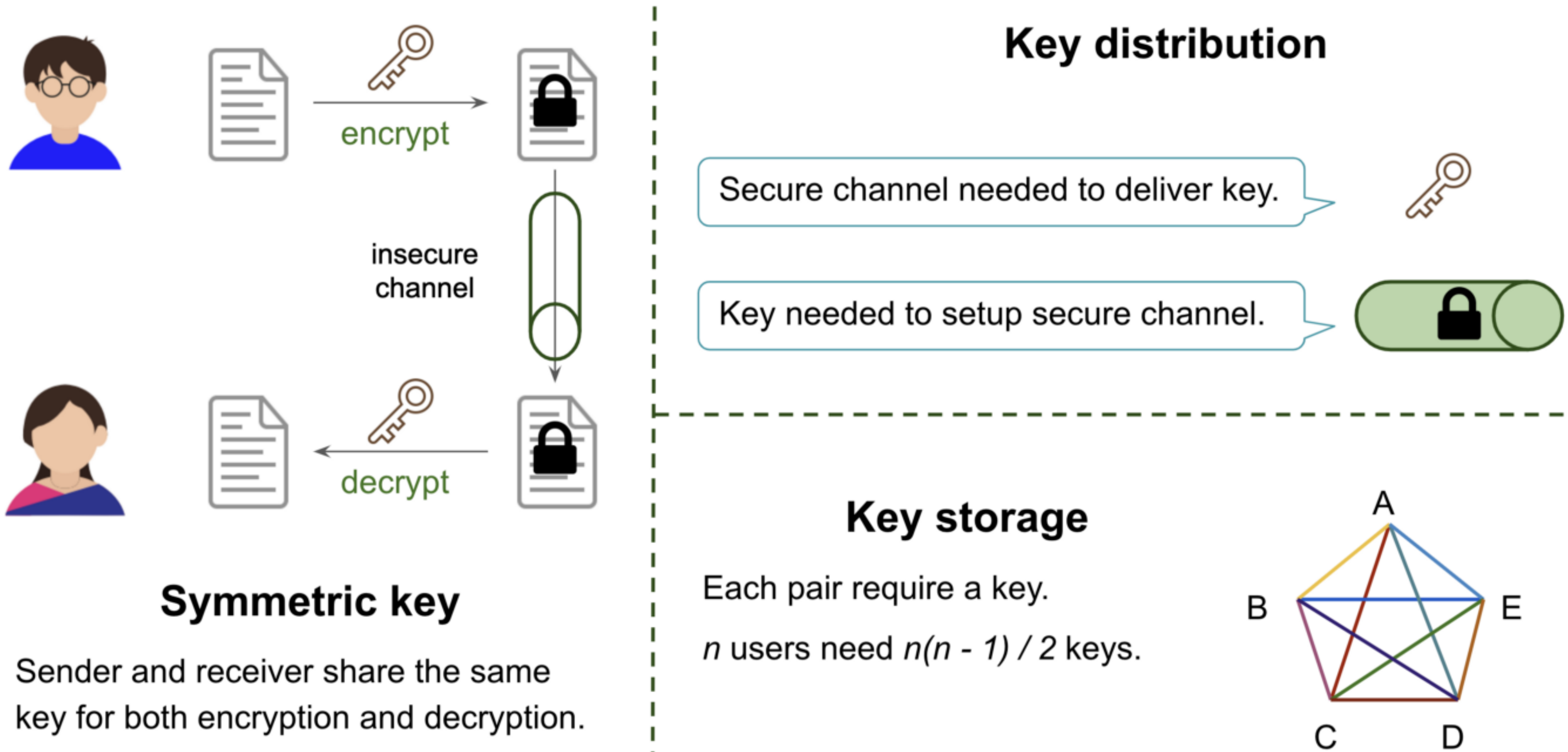


Strength of any cryptographic system rest with the *key distribution technique* !

Objective:

- delivering a key to two parties who wish to exchange data without allowing others to see the key

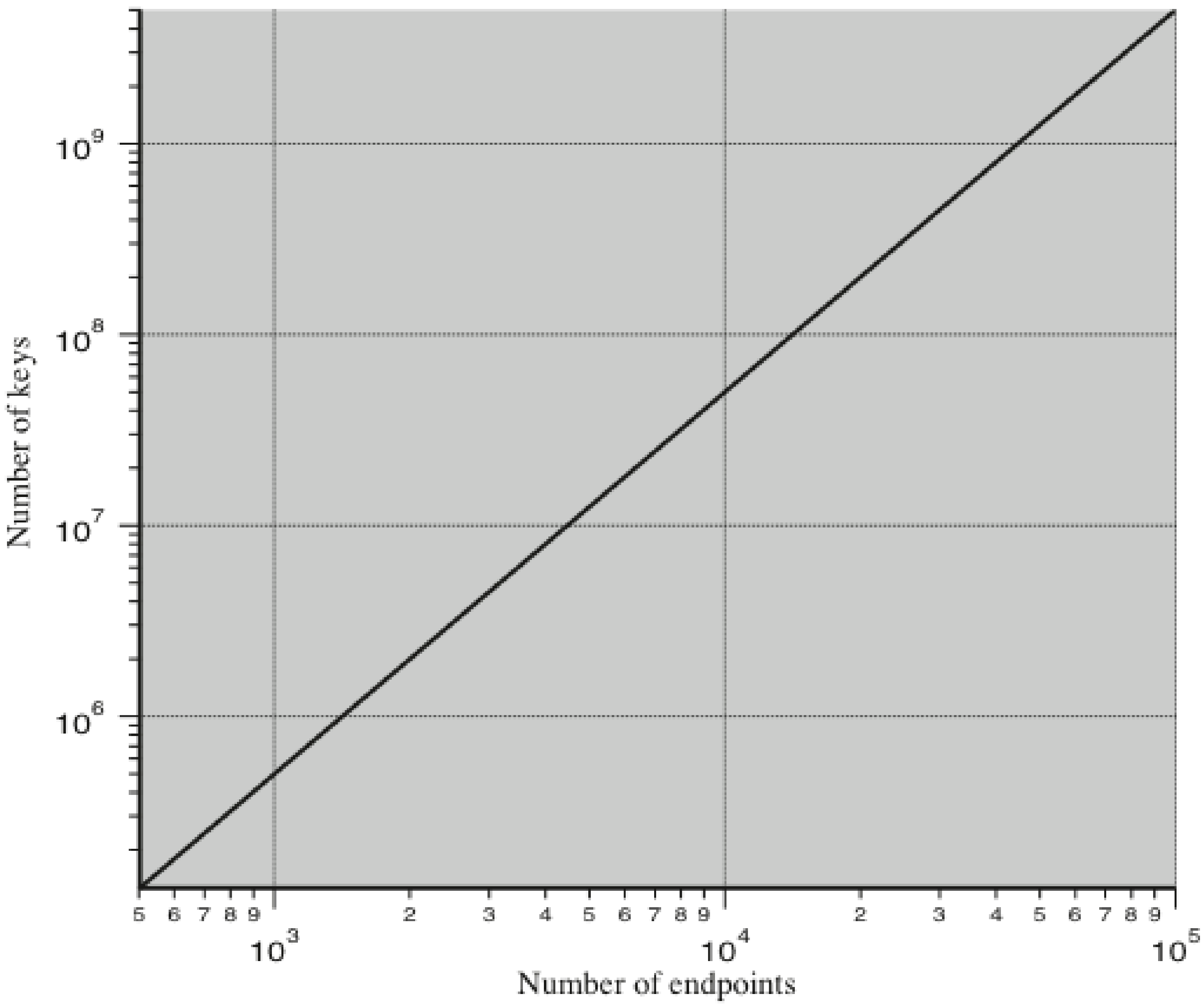
Key Distribution Challenges



If the encryption is done for each application, then a key is required for every pair of processes!

Source: https://kyle-crypto.medium.com/symmetric-asymmetric-encryption-5d8d4f6d80f1

Scale of the Problem



This figure illustrates the **magnitude of the key distribution** task for end-to-end encryption.

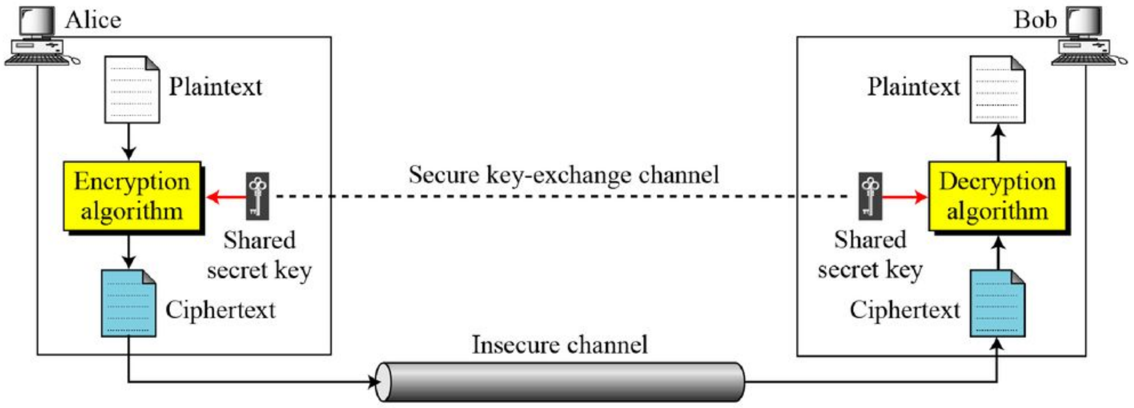
If a network supports 10,000 applications, then as many as 50 million keys may be required for application-level encryption !

Source: Cryptography and Network Security – Principles and Practice, by William Stallings, 7th Edition, Pearson India, 2017

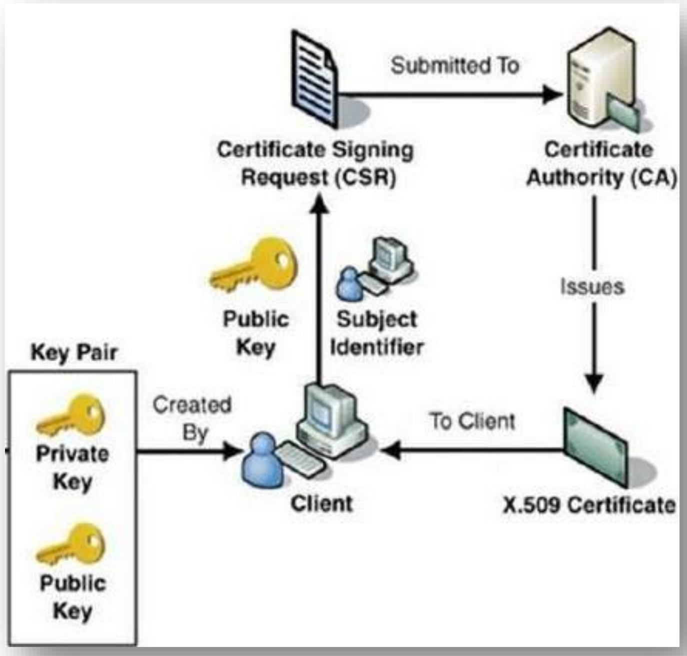
Key Distribution Technique

Type:

- Symmetric Key Distribution
  - Using Symmetric Encryption
  - Using Asymmetric Encryption



- Public Key Distribution
  - Using Public Announcement
  - Using Publicly Available Directory
  - Using Public-key Authority
  - Using Public-key Certificates



Source: https://www.google.com/

Symmetric Key Distribution

Given parties **A** and **B**, symmetric key distribution can be achieved in a number of ways:

Manual delivery

- **A** can select a key and physically deliver it to **B**
- A third party can select the key and physically deliver it to **A** and **B**

Network delivery

- If **A** and **B** have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key
- If **A** and **B** each has an encrypted connection to a third party **C**, **C** can deliver a key on the encrypted links to **A** and **B**

Cont…

Given parties **A** and **B**, symmetric key distribution can be achieved in a number of ways:

Network delivery

- If **A** and **B** have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key

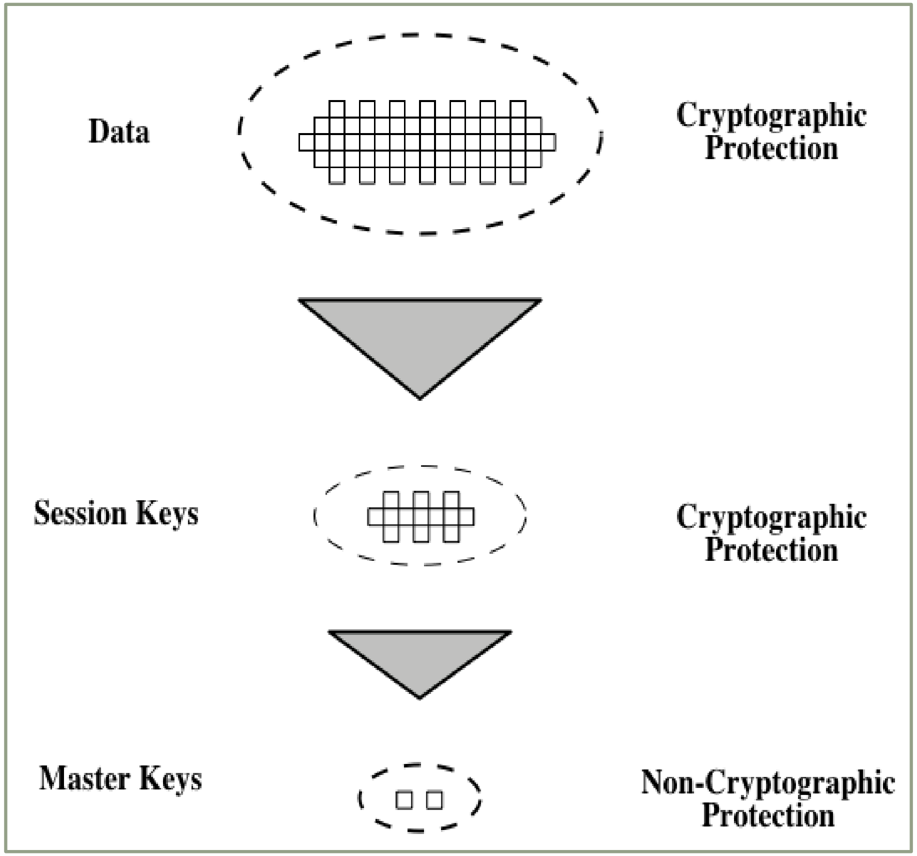
Disadvantages:

- if an attacker ever succeeds in gaining access to one key, then all subsequent keys will be revealed
- Initial distribution of millions of keys are challenging

- If **A** and **B** each has an encrypted connection to a third party **C**, **C** can deliver a key on the encrypted links to **A** and **B**

- **For end-to-end encryption, some variation on this option has been widely adopted**

Use of Key Hierarchy



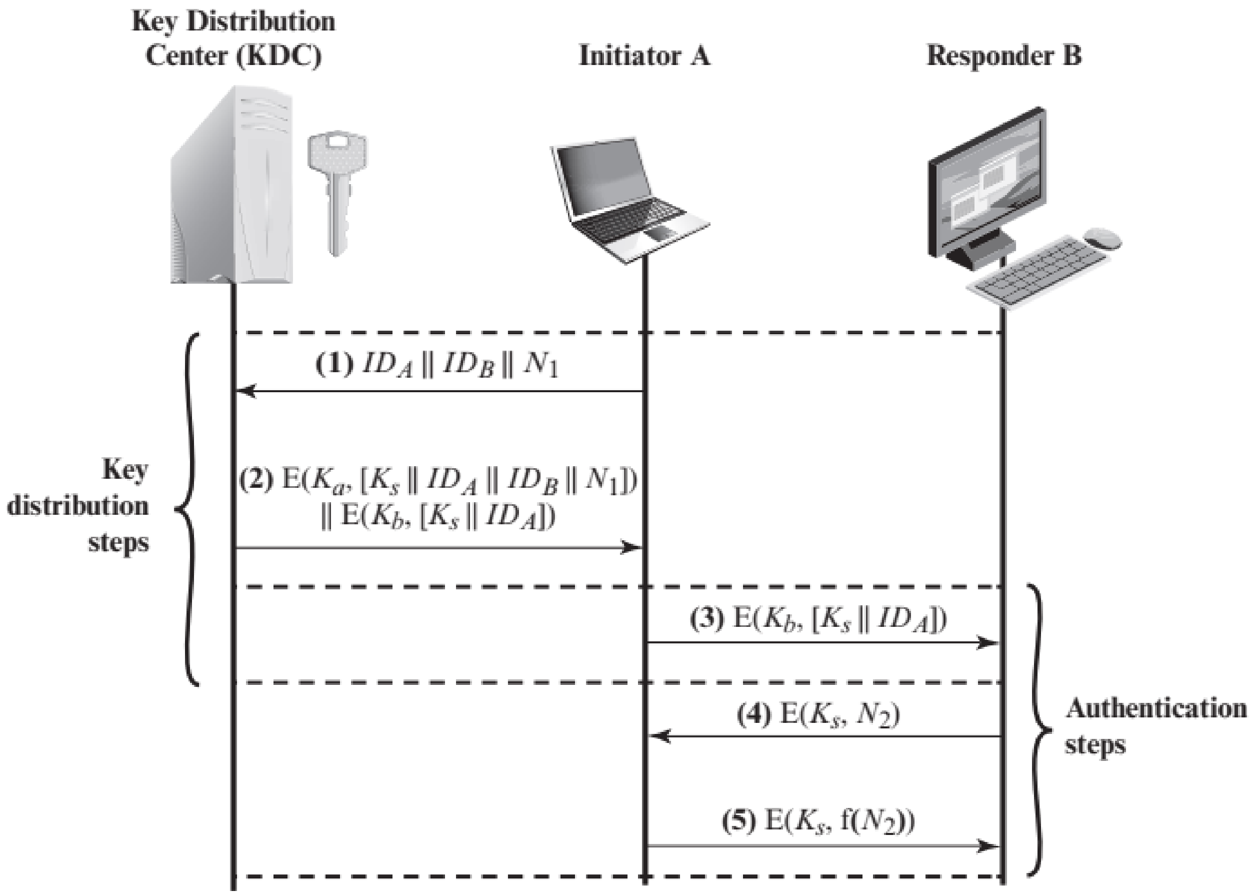
Use of Key Hierarchy

- In this last option, a key distribution centre (KDC) is responsible for distributing keys
- The use of a KDC is based on the use of a hierarchy of keys.
- Communication between end systems or users is encrypted using a temporary key, often referred to as a session key.
- Session keys are transmitted in encrypted form, using a master key
- For each end system or user, there is a unique master key that it shares with the KDC.
- Only N master keys are required for N users !

Source: Cryptography and Network Security – Principles and Practice, by William Stallings, 7th Edition, Pearson India, 2017

Key Distribution using Symmetric Encryption

Symmetric Key Distribution using Symmetric Encryption



K_a: Master key of A

K_b: Master key of B

K_s: One-time session key

ID_A: Identity of A

ID_B: Identity of B

N_1, N_2 : Nonce

E(.): Encryption

f(.): Do Some transformation

Ponder on:

What is the use of nonce?

Source: Cryptography and Network Security – Principles and Practice, by William Stallings, 7th Edition, Pearson India, 2017

Session Key Lifetime

For **connection-oriented protocols** one choice is to use the **same session key** for the **length of time** that the connection is open; and using a new session key for each new session

A security manager must balance the competing considerations.

For a **connectionless protocol** there is no explicit connection initiation or termination, thus **it is not obvious** how often one needs to change the session key

The more frequently session keys are exchanged, the more secure they are

The distribution of session keys places a burden on network capacity and delays the start of any data exchange

Source: Cryptography and Network Security – Principles and Practice, by William Stallings, 7th Edition, Pearson India, 2017

Decentralized Key Distribution

Requirement:

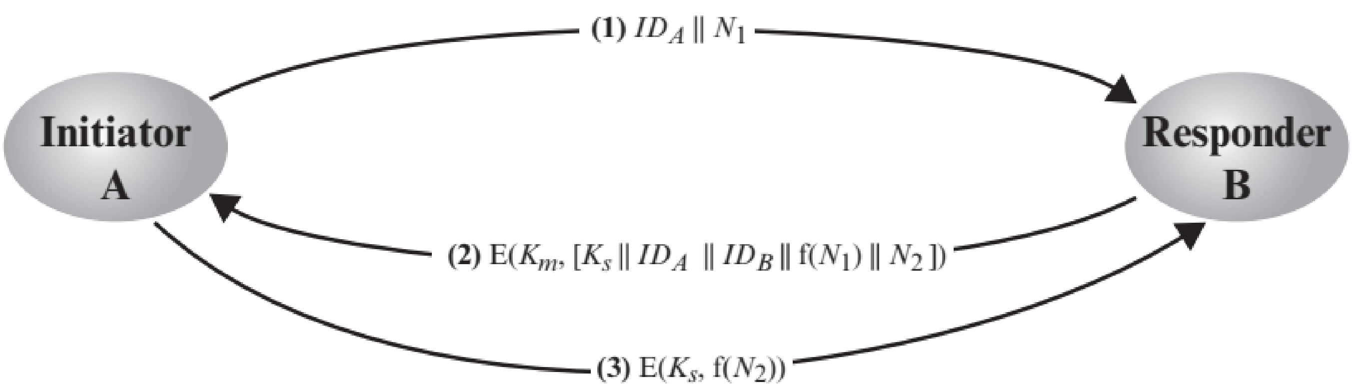
- the KDC needs to be trusted and be protected from subversion

Alternative:

- KDC is fully decentralized
  - For larger network, it is difficult using symmetric encryption
  - For local network, it is useful

A decentralized approach **requires that** each end-system be able to communicate in a secure manner with all partner end-systems for purposes of session key distribution.

- there may need to be as many as [n(n - 1)]/2 master keys for a configuration with n end-systems.



Source: Cryptography and Network Security – Principles and Practice, by William Stallings, 7th Edition, Pearson India, 2017

Controlling Key Usage

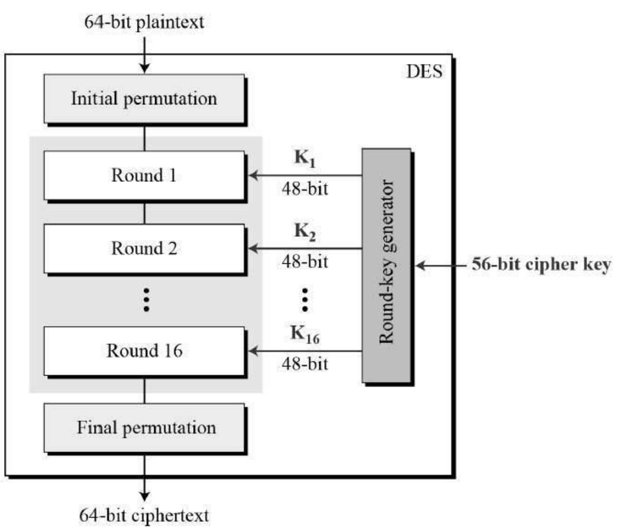
- The concept of a key hierarchy and the use of key distribution techniques greatly reduce the number of keys that must be managed and distributed.
- Requirement:
  - It may be desirable to impose some control on the way in which keys are used.
- For example:
  - We may wish to define different types of session keys on the basis of use, such as
    - ✓ Data-encrypting key -- for general communication across a network
    - ✓ PIN-encrypting key -- for PINs used in electronic funds transfer and point-of-sale (PoS) applications
    - ✓ File-encrypting key -- for the files stored in publicly accessible locations

Solution: Associate a tag with each key

Example: Eight non-key bits ordinarily reserved for parity checking in 64-bit DES key form the 8-bit key tag for DES

Bits have the following interpretation:

- whether the key is a session key or a master key
- whether the key can be used for encryption
- whether the key can be used for decryption
- remaining 5 bits are reserved for future use



Cont…

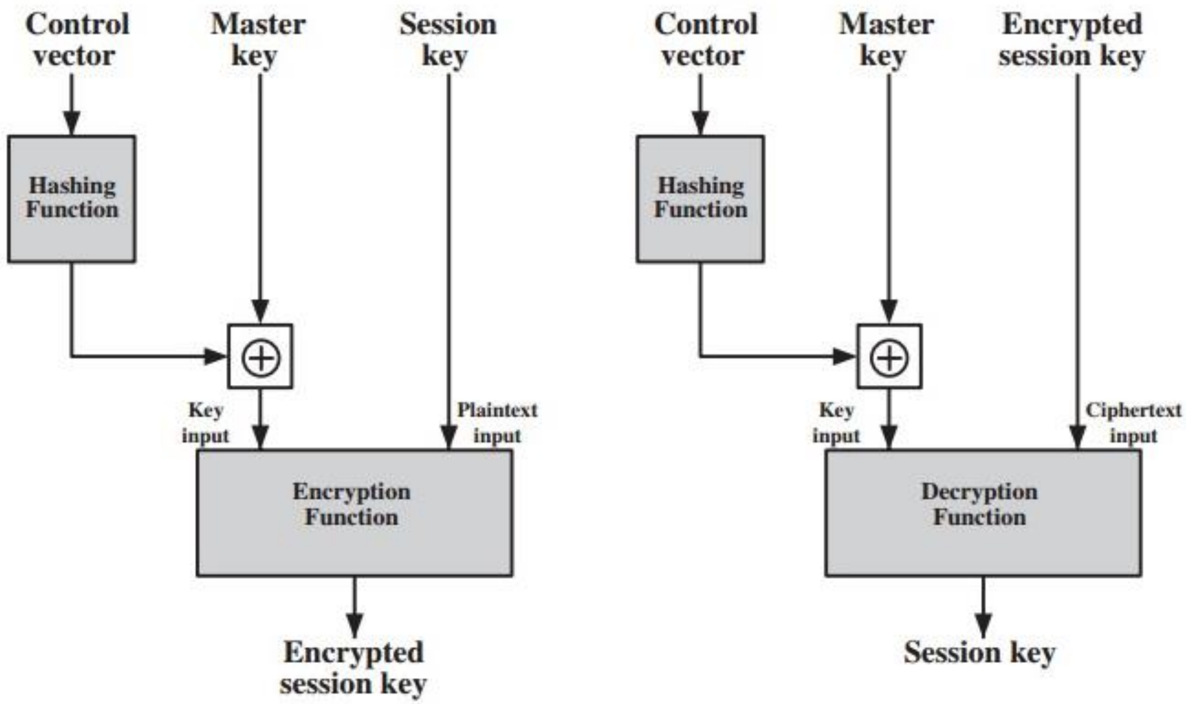
- The drawbacks of this tag-based scheme:
  - The tag length is limited to 8 bits
    - limiting its flexibility and functionality.
  - Because the tag is not transmitted in clear form, it can be used only at the point of decryption
    - limiting the ways in which key use can be controlled

A more flexible scheme: control vector

- The control vector is cryptographically coupled with the key at the time of key generation at the KDC.
- When a session key is delivered to a user from the KDC, it is accompanied by the control vector in clear form.

Cont…

- The coupling and decoupling processes are illustrated in the Figures

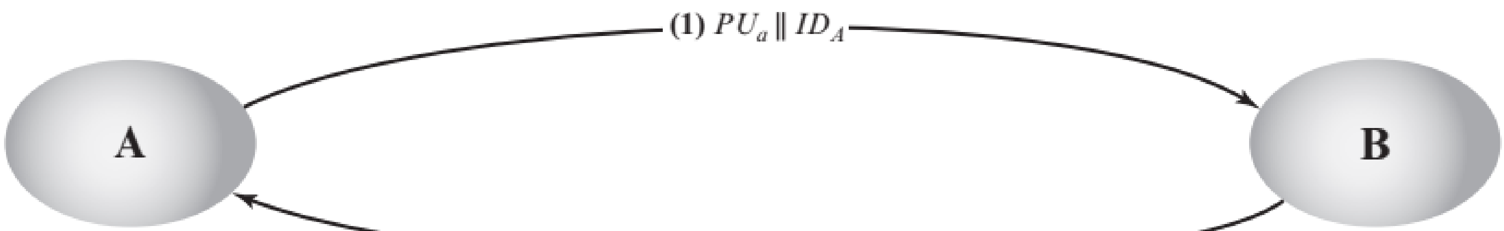


(a) Control vector encryption

(b) Control vector decryption

Key Distribution Using Asymmetric Encryption

An extremely simple scheme for Secret Key Distribution:



Public/Private Key pair:
[PU_a, PR_a]

Secret Key
K_s

- No keys exist before the start of communication and none exist after the completion of communication.
- Thus, the risk of compromise of the keys is minimal.

Disadvantages:

- Insecure for Man-In-The-Middle (MITM) attack
  - Adversary can either reply the intercepted message or substitute another message

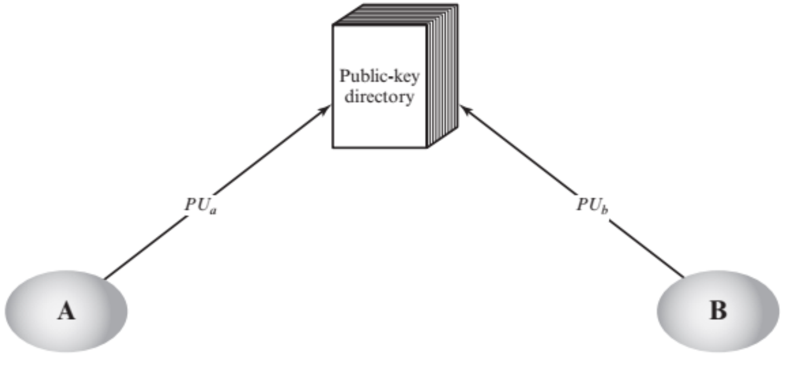
Source: Cryptography and Network Security – Principles and Practice, by William Stallings, 7th Edition, Pearson India, 2017

Distributions of Public Keys

- **Public Key Distribution**
  - Using Public Announcement
  - Using Publicly Available Directory
  - Using Public-key Authority
  - Using Public-key Certificates

Major weakness:

- Anyone can forge such a public announcement

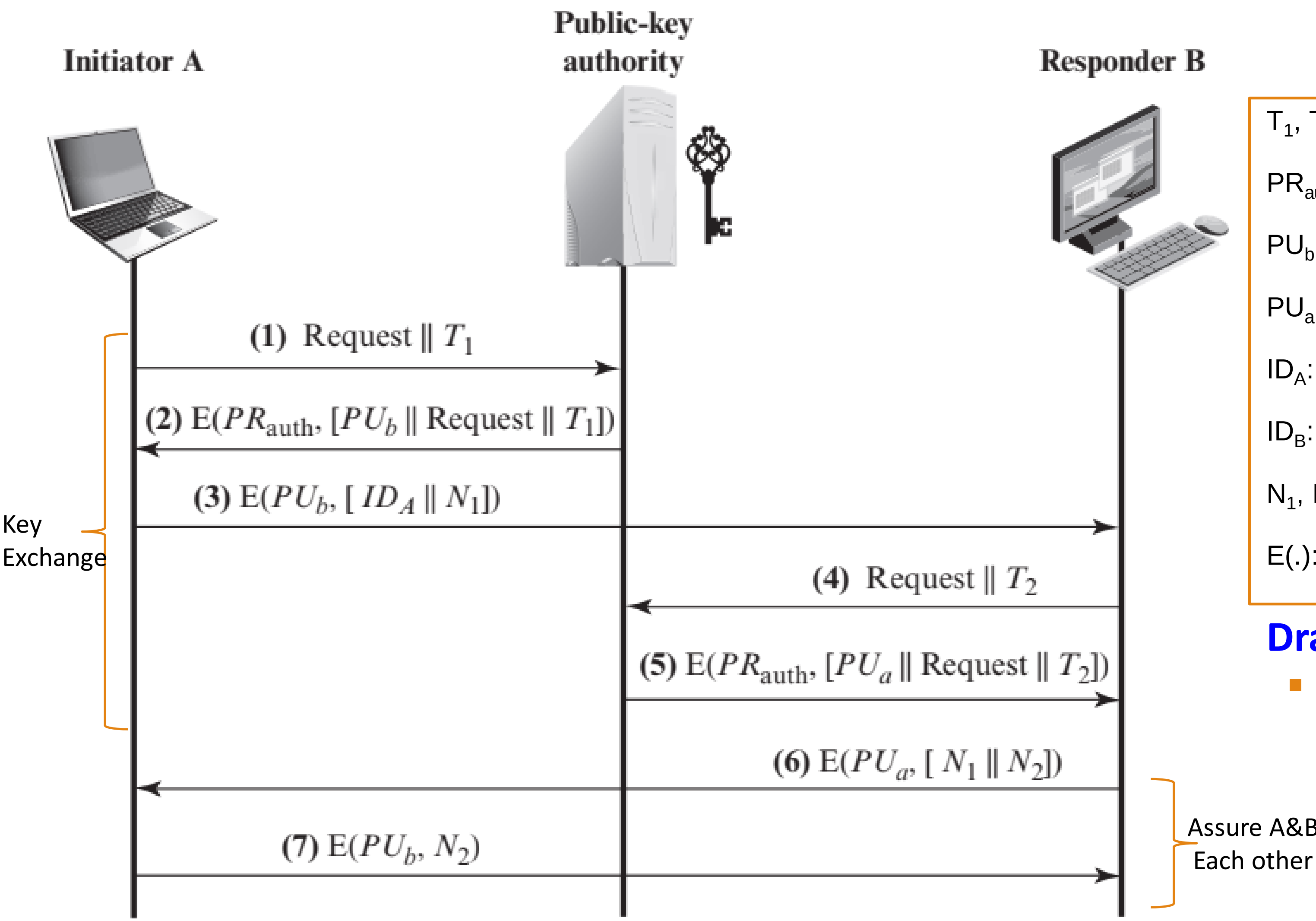


Major weakness:

- Single directory is the bottleneck
- Single key for long time

Source: Cryptography and Network Security – Principles and Practice, by William Stallings, 7th Edition, Pearson India, 2017

Public-key Authority



T_1, T_2: timestamped message

PR_{auth}: Authority's private key

PU_b: Public key of B

PU_a: Public key of A

ID_A: Identity of A

ID_B: Identity of B

N_1, N_2 : Nonce

E(.): Encryption

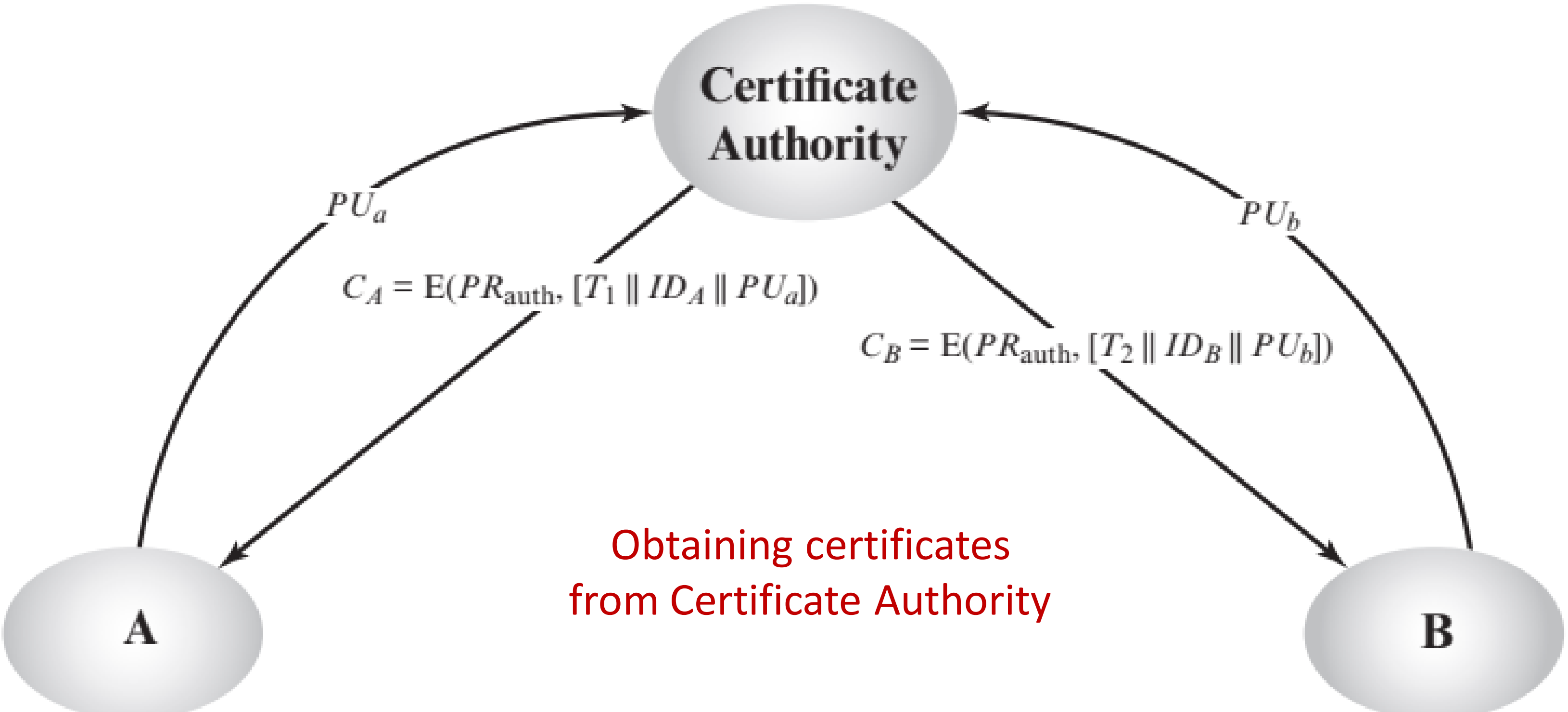
Drawbacks:

- Bottleneck in the system as every pair have to do this

Source: Cryptography and Network Security – Principles and Practice, by William Stallings, 7th Edition, Pearson India, 2017

Public-key Certificates

- ✓ **Certificates** will be used by the participants to exchange keys without contacting a public-key authority



Obtaining certificates
from Certificate Authority

Node A may pass this certificate to any other node who reads and verify the certificate as follows:

$$D(PU_{auth}, C_A) = D(PU_{auth}, E(PR_{auth}, [T \| ID_A \| PU_a])) = (T \| ID_A \| PU_a)$$

Cont…

Attributes:

- Any participant can read a certificate to determine the name and public key of the certificate's owner
- Any participant can verify that the certificate originated from the certificate authority and is not counterfeit.
- Only the certificate authority can create and update certificates.
- Any participant can verify the time validity of the certificate.

Points to Ponder:

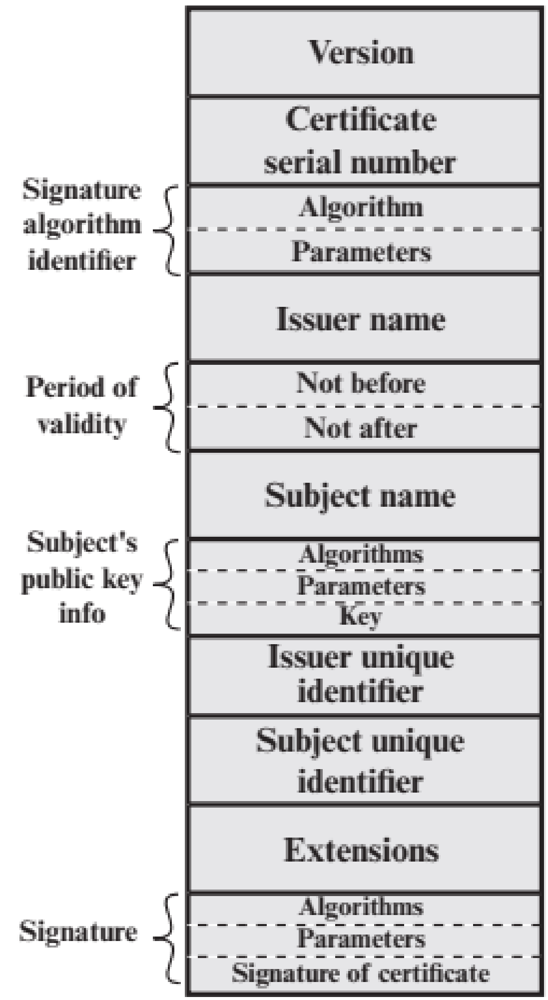
What is the use of timestamp T ?

Ans: The timestamp T validates the currency of the certificate.
In other words, the timestamp serves as something like an expiration date.

X.509 Certificates

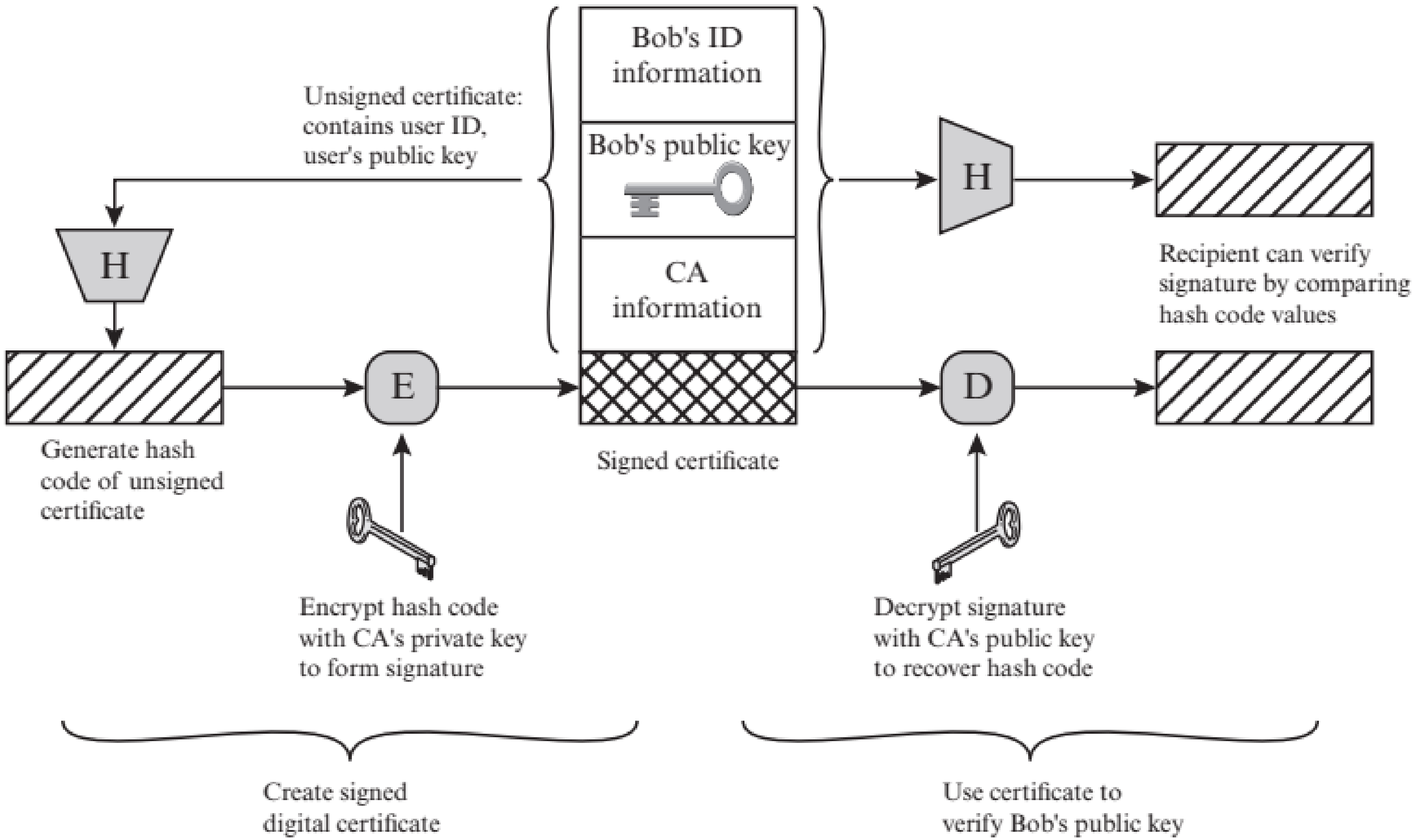
What is the format of a Public Key Certificate?

- ✓Universally accepted scheme for formatting public-key certificates: the X.509 standard
- ✓ X.509 defines a framework for the provision of authentication services to its users
  - ✓by the X.500 directory
  - ✓The directory is a server or distributed set of servers that maintains a database of information about users.
- ✓ X.509 is based on the use of public-key cryptography and digital signatures.
- ✓ Certificates are
  - ✓created by some trusted certification authority (CA),
  - ✓and placed in the directory by the CA or by the user.



General Format of a X.509 Certificate

X.509 Certificate Generation & Use



Certificate for Bob's Public Key

Source: Cryptography and Network Security – Principles and Practice, by William Stallings, 7th Edition, Pearson India, 2017

Certificate Revocation

- Each certificate includes a period of validity
  - ✓Typically a new certificate is issued just before the expiration of the old one

- It may be desirable on occasion to revoke a certificate before it expires, for one of the following reasons:
  - ✓The user's private key is assumed to be compromised
  - ✓The user is no longer certified by this CA
  - ✓The CA's certificate is assumed to be compromised

- Each CA must maintain a list consisting of all revoked but not expired certificates issued by that CA
  - ✓These lists should be posted on the directory

Public-Key Infrastructure (PKI)

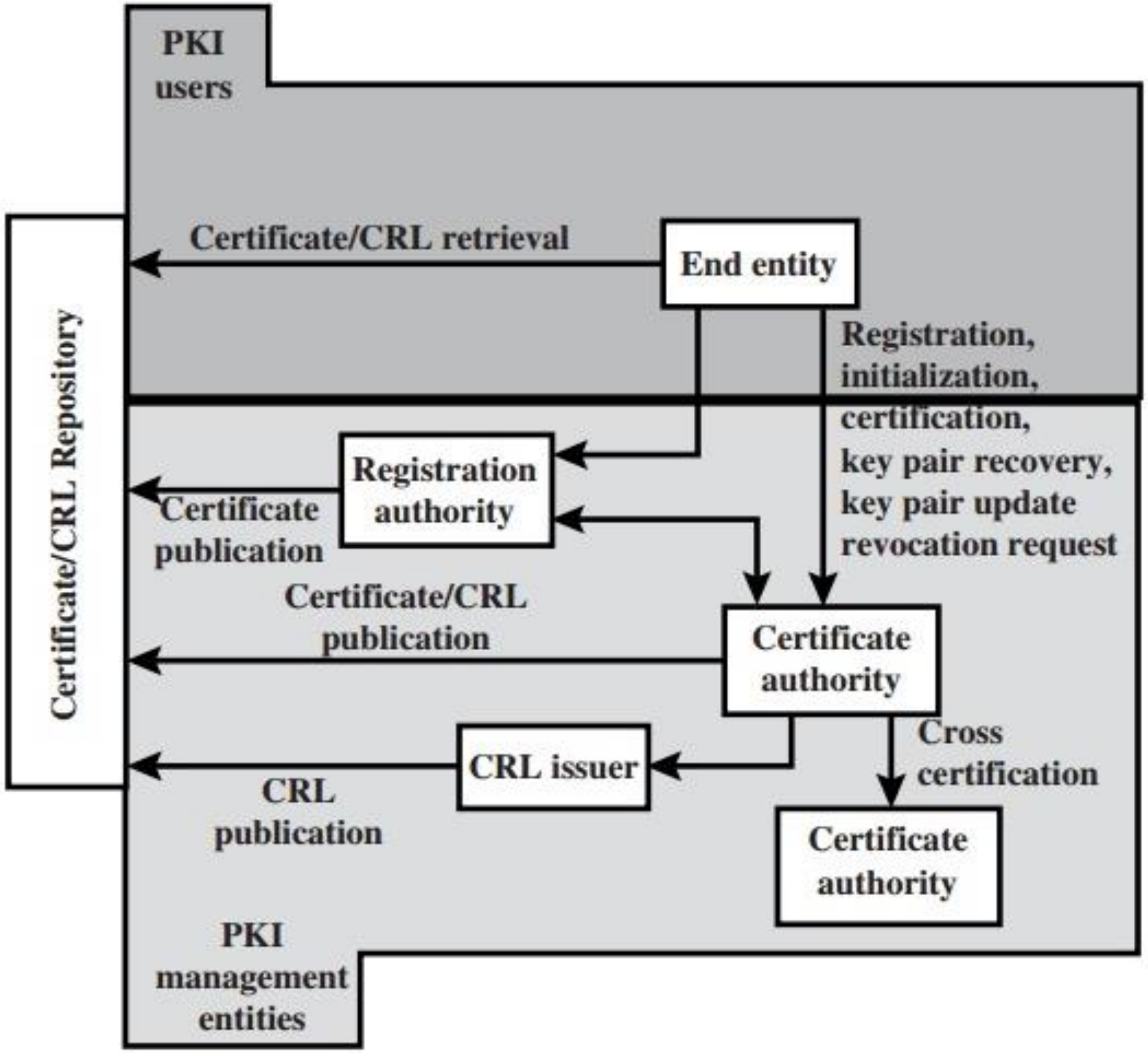
- Principal objective of PKI:
  - enable secure, convenient, and efficient acquisition of public keys.
  - create, manage, store, distribute and revoke digital certificates based on asymmetric cryptography

- IETF's Public Key Infrastructure X.509 (PKIX) working group has been the driving force behind setting up a formal (and generic) model based on X.509

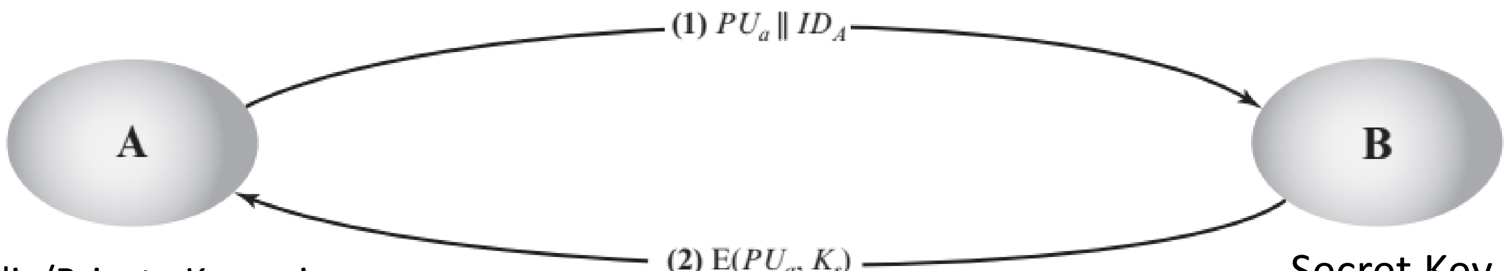
- It is suitable for deploying a certificate-based architecture on the Internet

- PKIX identifies different management functions
  - Registration -- a user makes itself known to CA for the first time
  - Initialization -- clients need to be initialized with the public keys of trusted CAs
  - Certification -- CA issues a certificate for a user's public key
  - Key pair recovery -- provide a mechanism to recover decryption keys when normal access to keying material is no longer available
  - Key pair update -- replaced with a new key pair
  - Revocation request -- authorized person do request to CA for certificate revocation
  - Cross certification -- is a certificate issued by one CA to another CA

PKIX Architectural Model



MITM Attack on Sym. Key Dist.



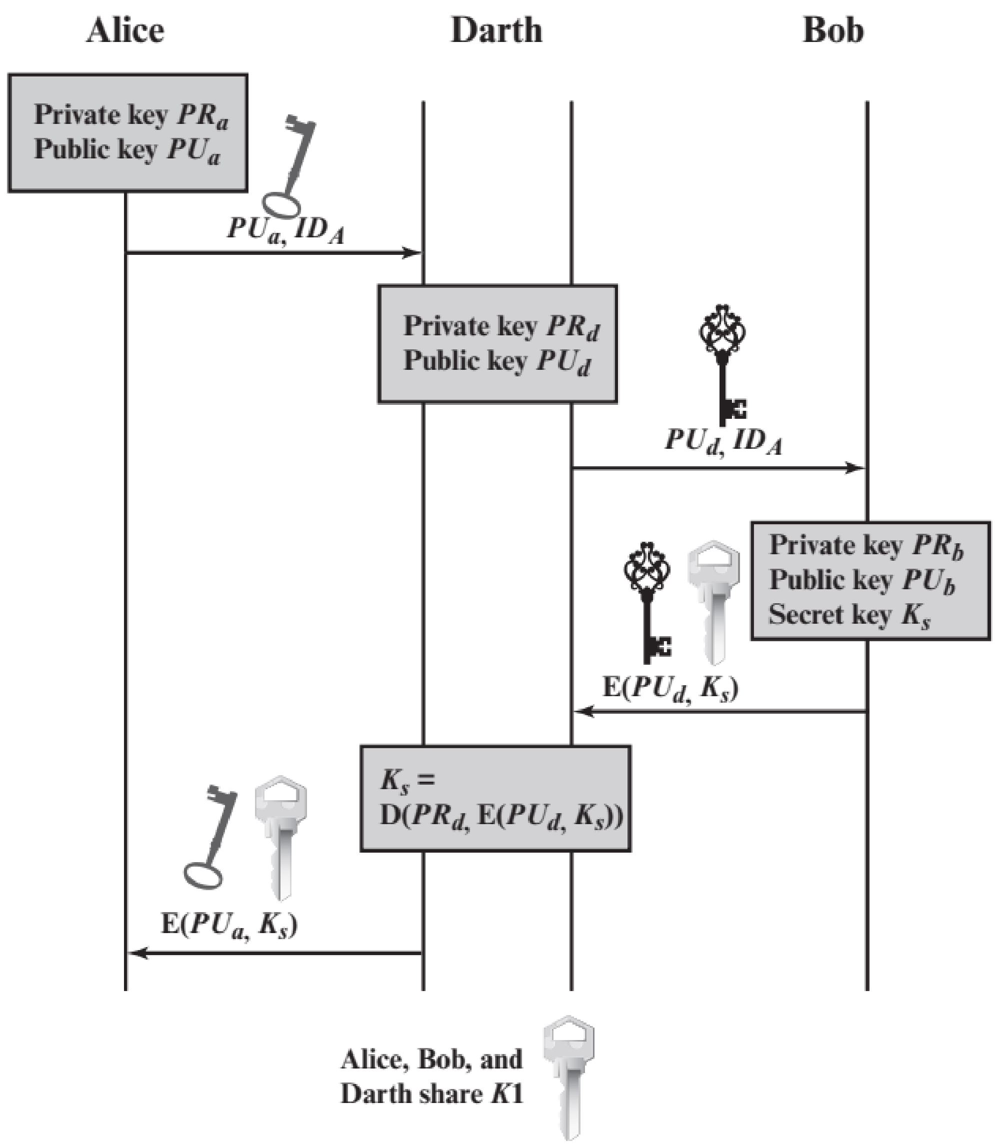
Public/Private Key pair:
[PU_a, PR_a]

Secret Key
K_s

<u>Man-in-the-Middle Attack</u> on <u>Symmetric Key Distribution using Asymmetric Encryption</u>

- Both A and B know K_s and are unaware that K_s can also be revealed to others (say D).
- A and B can now exchange messages using K_s.
- Knowing K_s, D can decrypt all messages, and both A and B are unaware of the problem.

Cont…

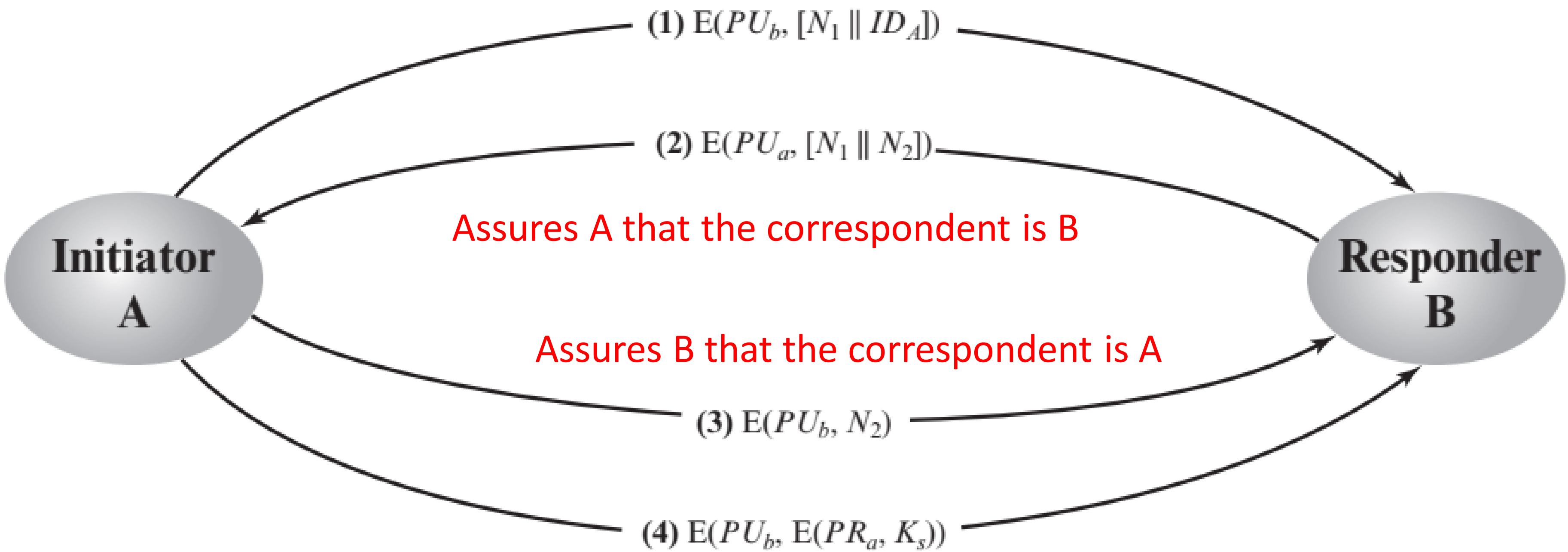


Alice
Darth
Bob
Private key PR_a
Public key PU_a
PU_a, ID_A
Private key PR_d
Public key PU_d
PU_d, ID_A
Private key PR_b
Public key PU_b
Secret key K_s
E(PU_d, K_s)
K_s =
D(PR_d, E(PU_d, K_s))
E(PU_a, K_s)
Alice, Bob, and
Darth share $K1$

Solution

Secret Key Distribution with **Confidentiality** and **Authentication**

N1 is used to identify this transaction uniquely



Ensures that only B can read it

Also ensures that only A could have sent it

Source: Cryptography and Network Security – Principles and Practice, by William Stallings, 7th Edition, Pearson India, 2017

Discrete Logarithms in Key Exchange

Objective in Key exchange:

- Enable two users to securely exchange a key that can then be used for subsequent symmetric encryption of messages

Effectiveness:

- Its effectiveness depends on the difficulty of computing discrete logarithms

Discrete Logarithm:

- Primitive root of a prime number p
  - It is one root whose powers modulo p generate all the integers from 1 to $p - 1$ in some permutation
  - If a is a primitive root of the prime number p, then the numbers

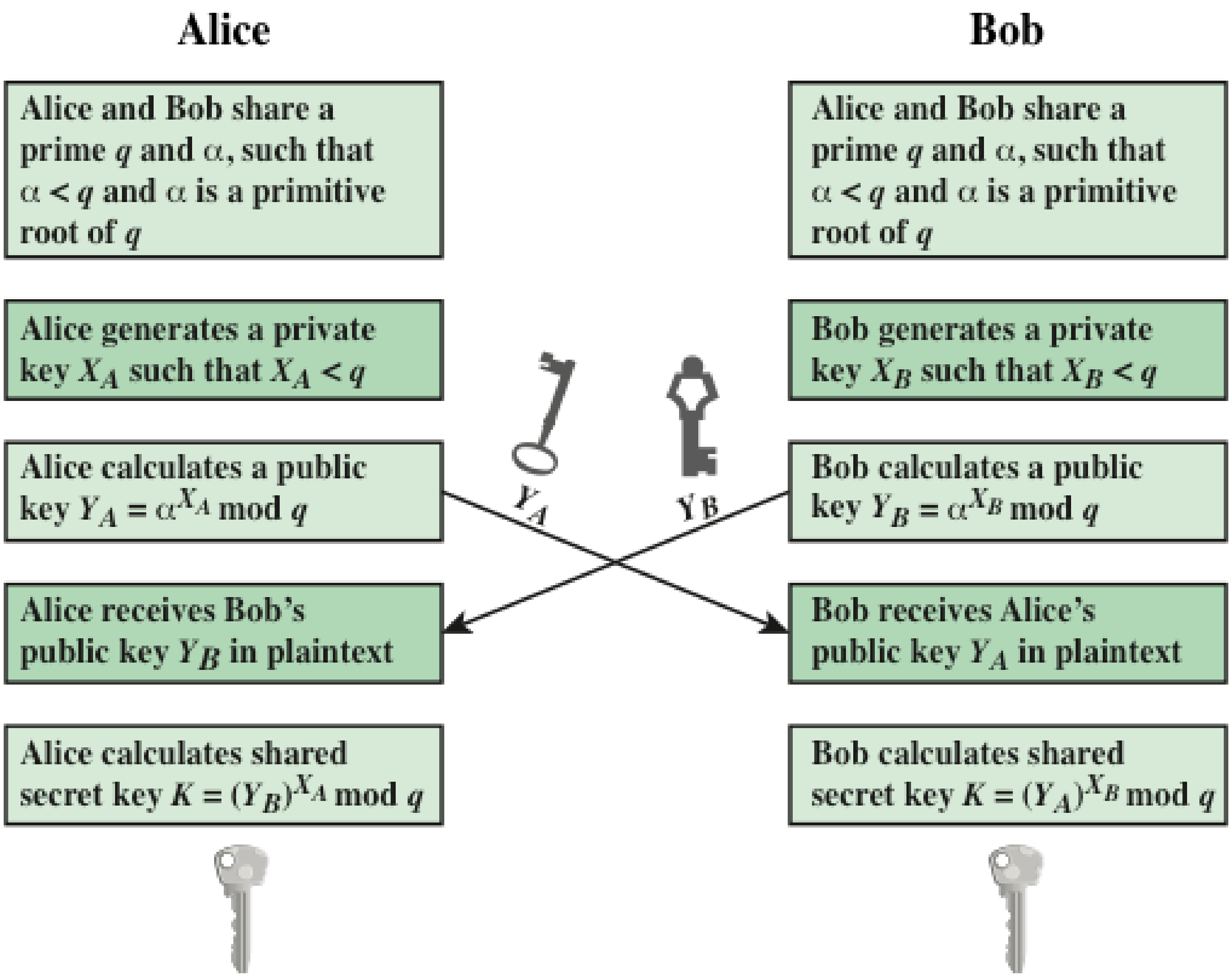
    $a \bmod p, a^2 \bmod p, \ldots, a^{p-1} \bmod p$

    are distinct and consist of the integers from 1 through p - 1 in some permutation.

- For any integer b and a primitive root a of prime number p
  - we can have a unique exponent i such that

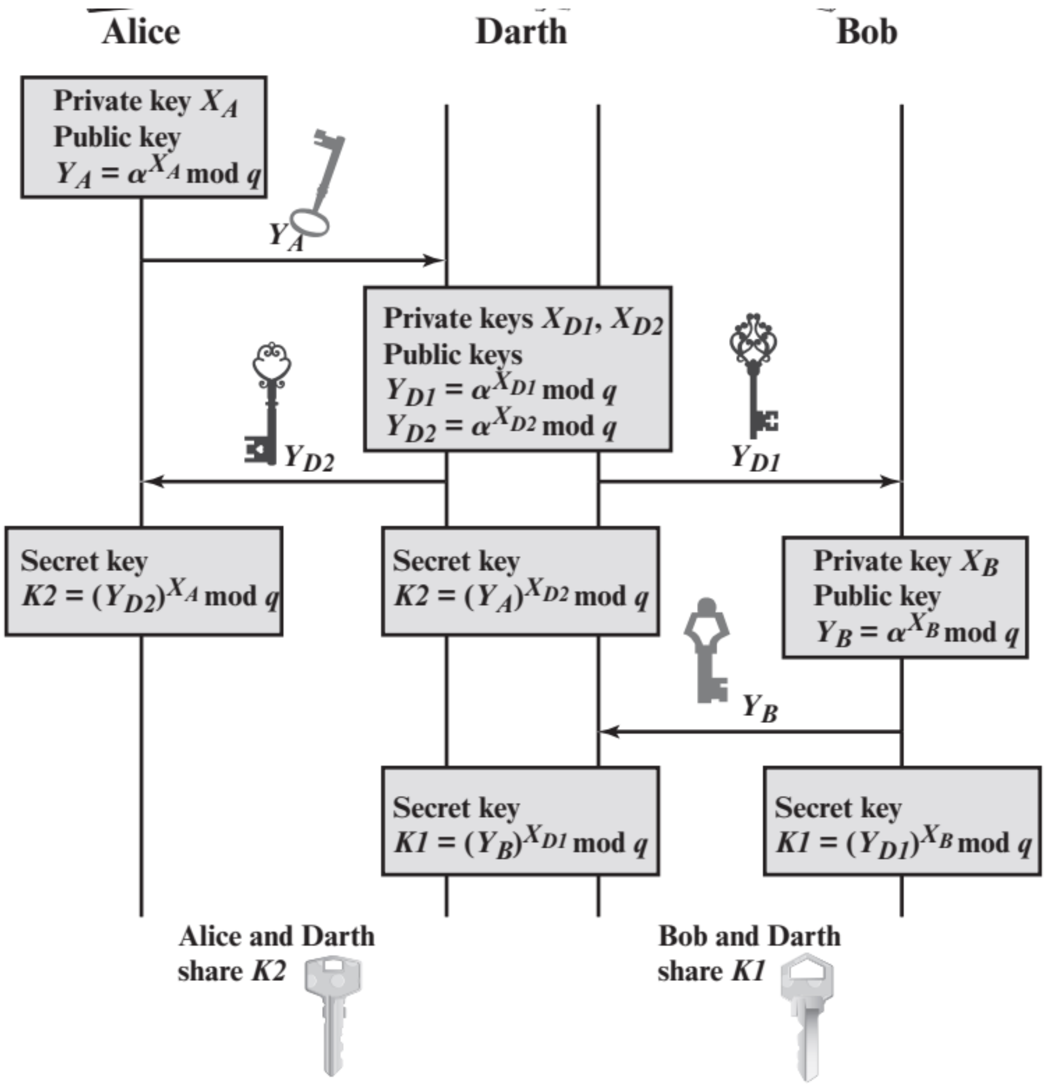
    $b = a^i \bmod p$ where $0 <= i <= (p - 1)$
  - The exponent i is referred to as the **discrete logarithm** of b for the base a, mod p.

Diffie-Hellman Key Exchange



Source: Cryptography and Network Security – Principles and Practice, by William Stallings, 7th Edition, Pearson India, 2017

MITM Attack on DH



Reason:

The key exchange protocol is vulnerable to such an attack because it does not authenticate the users.

Solutions:

Digital signatures and public-key certificates

A **valid digital signature**, gives a recipient very high confidence that

- the message was created by a known sender (authenticity),
- the message was not altered in transit (integrity).

A **public key certificate**, also known as a digital certificate that

- is used to prove the validity of a public key.

Source: Cryptography and Network Security – Principles and Practice, by William Stallings, 7th Edition, Pearson India, 2017

Thank you

Questions and Discussion