Computer System Security

Assoc. Prof. Noha A. Hikal

Information Technology Dept.

Faculty of Computers and Information Sciences

Subject Code:IT424

4th level –IT&IS

Week 6-18 March 2020

Outlines:

1. Quick reminder
2. Asymmetric Cryptography
3. Key management

1. Quick Reminder

Some Basic Terminology

- **plaintext** - original message
- **ciphertext** - coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering plaintext from ciphertext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis

Cryptography

Cryptographic system can be categorized by:

- Type of encryption operations used
  1. Substitution
  2. Transposition
  3. Product
- Number of keys used
  1. Single-key or private
  2. Two-key or public
- Way in which plaintext is processed
  1. Block
  2. Stream

Symmetric & Asymmetric Cryptography

Symmetric Enc. System

- AKA Private Key or Secrete Key
- Key must remain secrete to ensure authenticity for the source and the content.
- Exchanging Keys is an issue as the number of users increase. For n users:

$$\frac{n(n-1)}{2}$$

Keys required.

<u>Key Distribution</u> is an issue.

Asymmetric Enc. System

- AKA Public key
- Keys are produced together or one is derived from the other one mathematically.
- Key management excel here.

- When keys compromised, a key management is a major issue.

- AKA Private Key or Secrete Key
- Key must remain secrete to ensure authenticity for the source and the content.
- Exchanging Keys is an issue as the number of users increase. For n users:

$$\frac{n(n-1)}{2}$$

Keys required.

Key Distribution is an issue.

Symmetric Cryptography:

➨ **Substitution methods:**

1. Ceaser cipher
2. Playfair cipher

➨ **Transposition methods**

1. Row transposition, Block transposition
2. Railfence method

➨ **Product method**

1. DES, 2DES, 3DES
2. AES

Stream vs Block Ciphers

Stream cipher

- Message is encrypted in bits or bytes
- Usable for real time applications.

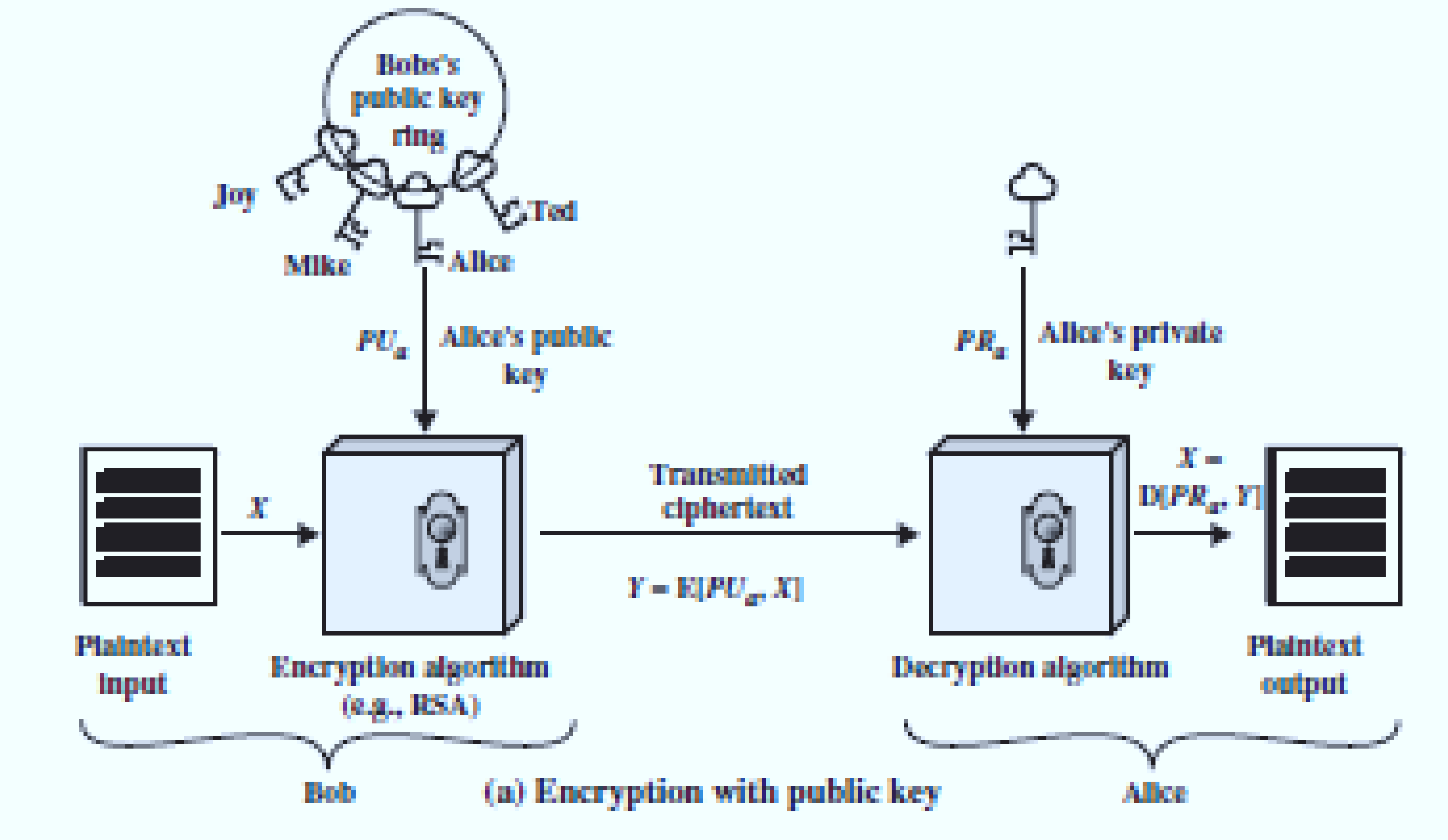
Block cipher

- Message is broken into fixed size blocks and each block is encrypted.
- Padding is used for short blocks

	Stream	**Block**
Speed of transformation	Fast	Slow
Error propagation	Low	High
Padding	No	Yes
Immunity to insertion of symbols	No	Yes

2. Asymmetric Cryptography

Asymmetric Cryptography



(a) Encryption with public key

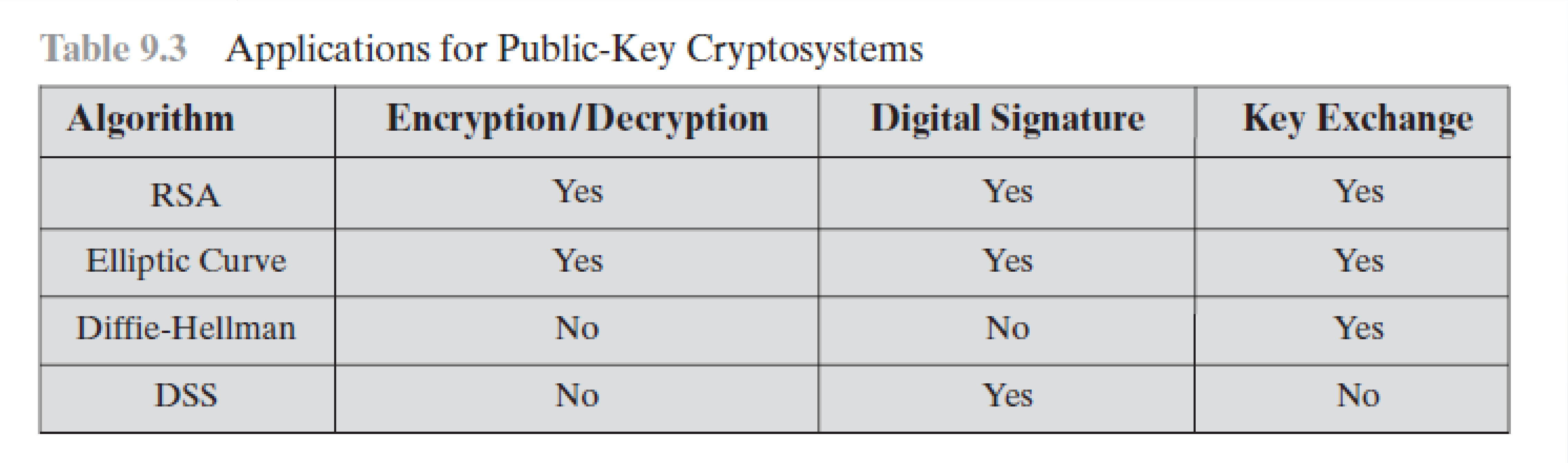


Table 9.3 Applications for Public-Key Cryptosystems

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

Public-Key Cryptography limitations

- Can be used for secrecy or authentication
- Public-key algorithms are slow
- So usually want to use private-key encryption to protect message contents, Hence need a session key

3. Key Management

RECALL: Symmetric & Asymmetric Cryptography

Symmetric Enc. System

- AKA Private Key or Secrete Key
- Key must remain secrete to ensure authenticity for the source and the content.
- **Exchanging Keys is an issue as the number of users increase. For n users:**

$$\frac{n(n-1)}{2}$$

Keys required.

Key Distribution is an issue.

Asymmetric Enc. System

- AKA Public key
- Keys are produced together or one is derived from the other one mathematically.
- Key management excel here.

- **When keys compromised, a key management is a major issue.**

Key Management

key distribution refers to the procedures by which keys are securely provided to parties legitimately asking for them.

Public-key encryption helps address key distribution problems

Have two aspects of this:

- Distribution of public keys
- Use of public-key encryption to distribute secret keys

key management is a major issue. It involves storing, safeguarding, and activating keys

Distribution of Public Keys

- can be done using one of the following techniques:
  1. Public announcement
  2. Publicly available directory
  3. Public-key authority
  4. Public-key certificates

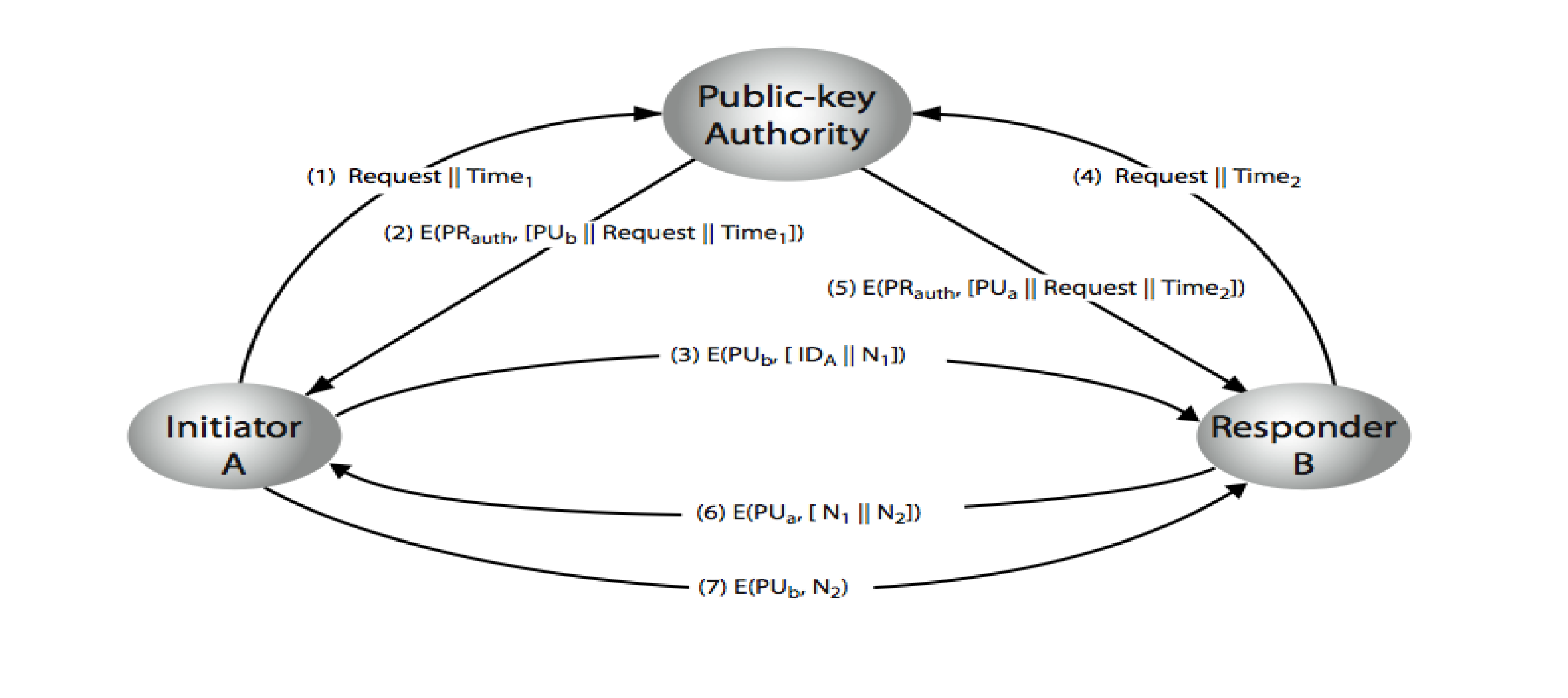
1- Public Announcement

- users distribute public keys to recipients or broadcast to community at large
  - eg. 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

2-Publicly Available Directory

- can obtain greater security by registering keys with a public directory
- directory must be trusted with properties:
  1. contains {name, public-key} entries
  2. participants register securely with directory
  3. participants can replace key at any time
  4. directory is periodically published
  5. directory can be accessed electronically
- still vulnerable to tampering or forgery

3-Public-Key Authority

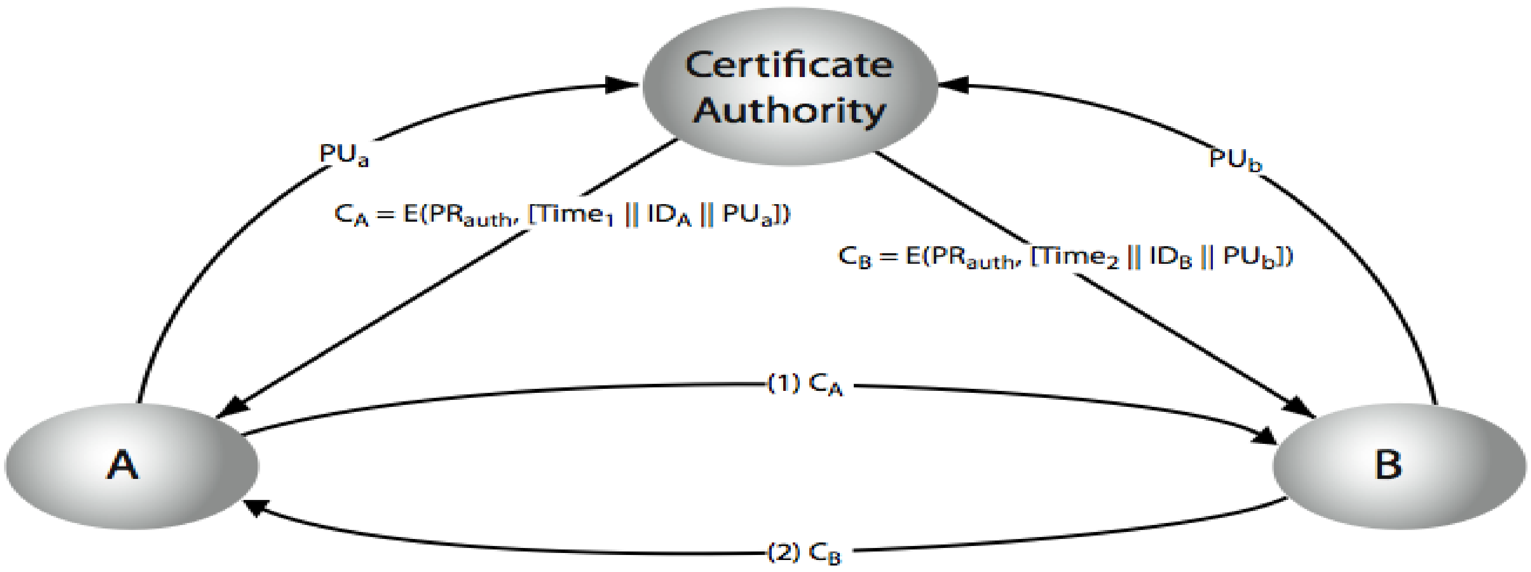

Public-key Authority
(1) Request || Time$_1$
(4) Request || Time$_2$
(2) E(PR$_{auth}$, [PU$_b$ || Request || Time$_1$])
(5) E(PR$_{auth}$, [PU$_a$ || Request || Time$_2$])
(3) E(PU$_b$, [ID$_A$ || N$_1$])
Initiator A
Responder B
(6) E(PU$_a$, [N$_1$ || N$_2$])
(7) E(PU$_b$, N$_2$)

Public-Key Authority (continued)

1. Improve security by tightening control over distribution of keys from directory
2. Has properties of directory
3. Requires users to know public key for the directory
4. Then users interact with directory to obtain any desired public key securely

   require real-time access to directory when keys are needed

4- Public-Key Certificates


Certificate Authority
PU_a
PU_b
$C_A = E(PR_{auth}, [Time_1 || ID_A || PU_a])$
$C_B = E(PR_{auth}, [Time_2 || ID_B || PU_b])$
A
B
(1) C_A
(2) C_B

Public-Key Certificates (continued)

1. Certificates allow key exchange without real-time access to public-key authority
2. A certificate binds **identity** to **public key**
    1. Usually with other info such as period of validity, rights of use etc
3. With all contents **signed** by a trusted public-key or certificate authority (CA)
4. Can be verified by anyone who knows the public-key authorities public-key

THANK YOU

Reference:

1. Textbook: Security in Computing, 5th Edition , 2015 by Charles P. Pfleeger.
2. Stallings W, Brown L, Bauer MD, Bhattacharjee AK. Computer security: principles and practice. Upper Saddle River, NJ, USA: Pearson Education; 2012.
3. Internet resources.