CHƯƠNG 3 – ĐẢM BẢO AN TOÀN THÔNG TIN DỰA TRÊN MÃ HÓA

3.1. Khái quát về mã hóa thông tin và ứng dụng

3.2. Mã hóa cổ điển

3.3. Các hệ mã hóa khóa đối xứng

3.4. Các hệ mã hóa khóa bất đối xứng

3.5. Chữ ký số, chứng chỉ số và PKI

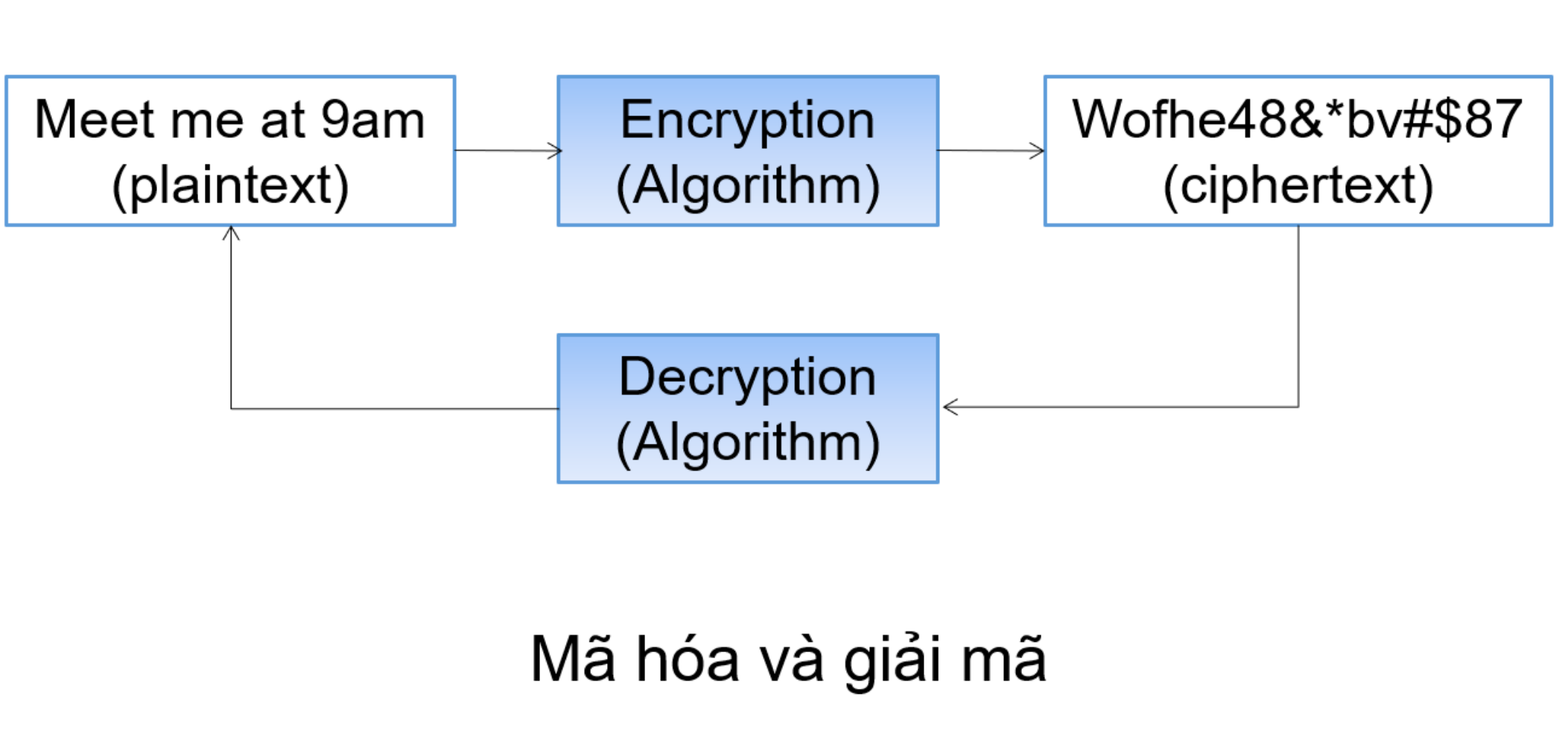
3.6. Quản lý khóa và phân phối khóa

3.1. Khái quát về mã hóa thông tin và ứng dụng

Mã hóa thông tin là gì?

- Định nghĩa theo Webster's Revised Unabridged Dictionary: cryptography is "the act or art of writing secret characters" – mật mã là một hành động hoặc nghệ thuật viết các ký tự bí mật.
- Định nghĩa theo Free Online Dictionary of Computing: cryptography is "encoding data so that it can only be decoded by specific individuals." – mật mã là việc mã hóa dữ liệu mà nó chỉ có thể được giải mã bởi một số người chỉ định.
- Một hệ mã hóa gồm 2 khâu:
  - Mã hóa (encryption)
  - Giải mã (decryption)

3.1. Khái quát về mã hóa thông tin và ứng dụng



Mã hóa và giải mã

3.1. Khái quát về mã hóa thông tin và ứng dụng

Các thuật ngữ

- Thông tin chưa được mã hóa (Unencrypted information) là thông tin ở dạng có thể hiểu được.
  - Cũng được gọi là bản rõ (plaintext hay cleartext)
- Thông tin đã được mã hóa (Encrypted information) là thông tin ở dạng đã bị xáo trộn.
  - Cũng được gọi là bản mã (ciphertext hay encrypted text)
- Mã hóa (Encryption) là hành động xáo trộn (scrambling) bản rõ để chuyển thành bản mã.
- Giải mã (Decryption) là hành động giải xáo trộn (unscrambling) bản mã để chuyển thành bản rõ.

3.1. Khái quát về mã hóa thông tin và ứng dụng

Các thuật ngữ

- Một bộ mã hóa (Cipher) là một giải thuật để mã hóa và giải mã thông tin.
- Khóa/Chìa (Key) là một chuỗi/tham số được sử dụng trong giải thuật mã hóa và giải mã.
- Không gian khóa (Keyspace) là tổng số khóa có thể có của một hệ mã hóa.
- Phá mã/Thám mã (Cryptanalysis) là quá trình giải mã thông điệp đã bị mã hóa (ciphertext) mà không cần có trước thông tin về giải thuật mã hóa (Encryption algorithm) và khóa mã (Key).

3.1. Khái quát về mã hóa thông tin và ứng dụng

Các thuật ngữ

- Mã hóa dòng (Stream cipher) là kiểu mã hóa mà từng bít (hoặc ký tự) của dữ liệu được kết hợp với từng bít (hoặc ký tự) tương ứng của khóa để tạo thành bản mã.
- Mã hóa khối (Block cipher) là kiểu mã hóa mà dữ liệu được chia ra thành từng khối có kích thước cố định để mã hóa.

3.1. Khái quát về mã hóa thông tin và ứng dụng

Các thành phần của một hệ mã hóa

- Một hệ mã hoá (cryptosystem) được cấu thành từ hai thành phần chính:
  - Phương pháp mã hoá, còn gọi là "giải thuật" (Algorithm)
  - Một tập các khoá, còn gọi là không gian khoá (Keyspace)
- Nguyên lý Kerckhoff: "*tính an toàn của một hệ mã hoá không nên phục thuộc vào việc giữ bí mật giải thuật mã hoá, mà chỉ nên phục thuộc vào việc giữ bí mật khoá mã*".

3.1. Khái quát về mã hóa thông tin và ứng dụng

Vai trò của mã hóa trong ATTT

- Mã hoá thông tin có thể được sử dụng để đảm bảo an toàn thông tin trên đường truyền với các thuộc tính:
  - Bí mật (confidentiality): đảm bảo chỉ những người có thẩm quyền mới có khả năng truy nhập vào thông tin;
  - Toàn vẹn (integrity): đảm bảo dữ liệu không bị sửa đổi bởi các bên không có đủ thẩm quyền;
  - Xác thực (authentication): thông tin nhận dạng về các chủ thể tham gia phiên truyền thông có thể xác thực;
  - Không thể chối bỏ (non-repudiation): cho phép ngăn chặn một chủ thể chối bỏ hành vi hoặc phát ngôn đã thực hiện.

3.1. Khái quát về mã hóa thông tin và ứng dụng

Các tiêu chuẩn đánh giá hệ mã hóa

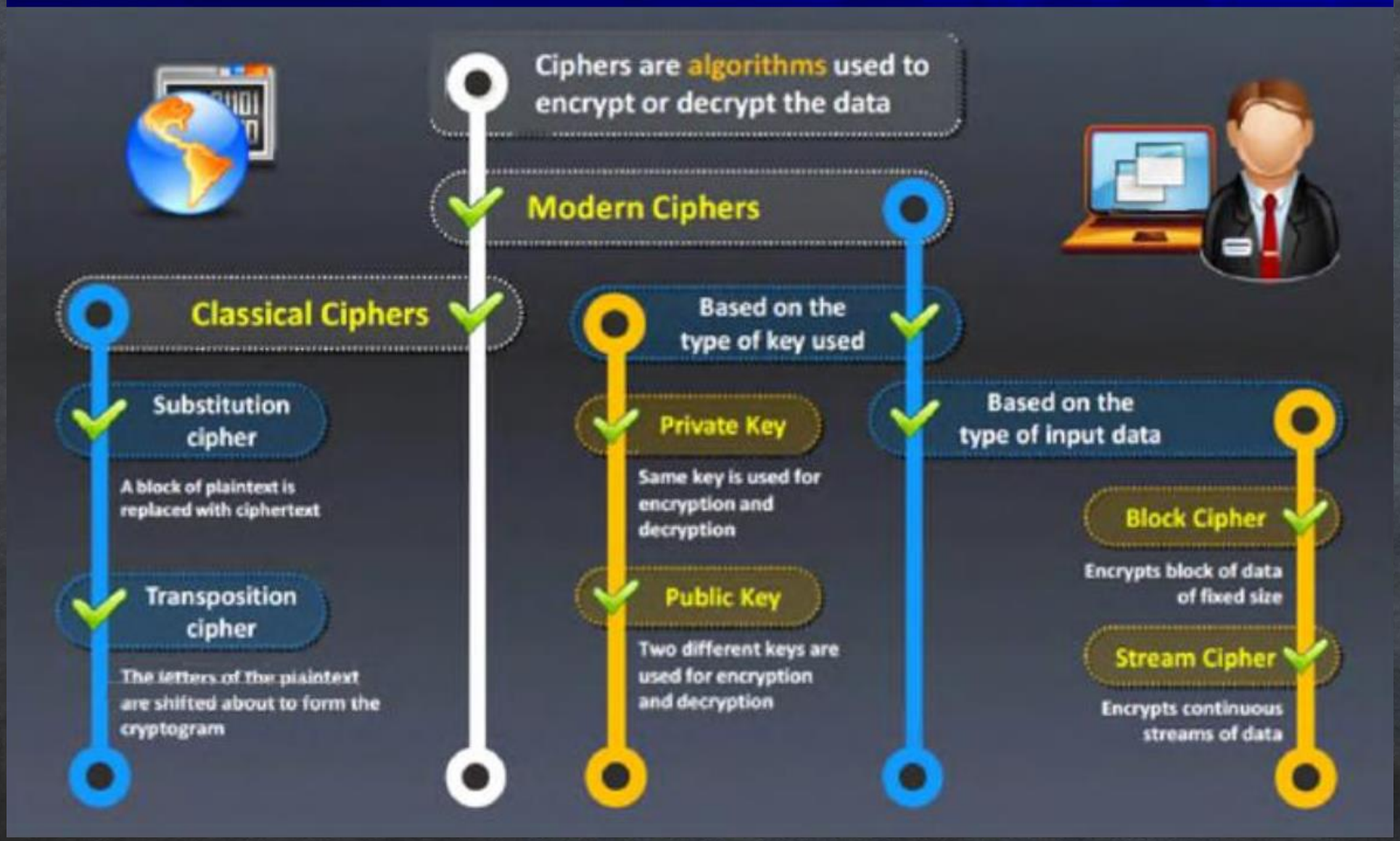
- **Độ an toàn** (level of security): thường được đánh giá thông qua số lượng tính toán để có thể phá được hệ mã hoá.
- **Tính năng** (functionality): hệ thống có thể được sử dụng cho nhiều mục đích bảo mật.
- **Chế độ hoạt động** (methods of operation): cung cấp các tính năng khác nhau theo chế độ hoạt động.
- **Hiệu năng** (performance): có thể được đo bằng tốc độ mã hoá (bits/giây).
- **Độ dễ cài đặt** (ease of implementation): độ khó của việc cài đặt thuật toán trong thực tế trên phần cứng hoặc phần mềm.

3.1. Khái quát về mã hóa thông tin và ứng dụng

Ứng dụng của mã hóa

- Các kỹ thuật mã hóa được ứng dụng rộng rãi trong các hệ thống/công cụ/dịch vụ bảo mật:
  - Dịch vụ xác thực (Kerberos, RADIUS,…)
  - Điều khiển truy cập
  - Các công cụ đánh giá và phân tích logs
  - Các sản phẩm quản lý ATTT
  - Các công cụ cho đảm bảo an toàn cho truyền thông không dây
  - Các nền tảng bảo mật như PKI, PGP
  - Các giao thức bảo mật như SSL/TLS, SSH, SET, IPSec
  - Các hệ thống như VPN.

3.2. Mã hóa cổ điển



3.2. Mã hóa cổ điển

3.2.1. Mã hoán vị bậc d

- Đối với một số nguyên dương d bất kỳ, chia thông báo m thành từng khối có chiều dài d.
- Khóa là một hoán vị h của 1, 2, …, d. Không gian khóa là d!
- Mã hóa bằng cách áp dụng h vào mỗi khối d kí tự của m
- VD: nếu d=5 và h=(4 1 3 2 5) tức là thứ tự (1 2 3 4 5) của nhóm d kí tự sẽ được thay thế bằng hoán vị mới h= (4 1 3 2 5)=khóa
- Cho m= hengapngaymai
  m =“ henga pngay mai..”
  12345 12345 12345

C= ghnea apgny .mia.

Kết luận: bản mã ghneaapgnymia

3.2. Mã hóa cổ điển

3.2.1. Mã hoán vị bậc d

- Giải mã
- VD: nếu d=5 và h=(4 1 3 2 5),
  Cho c= ghnea opavt ahbuy
  12345 12345 12345

Tìm p?

h = 4 1 3 2 5

1 2 3 4 5

4 1 3 2 5

h'= 2 4 3 1 5

P = henga pvaot hubay

KL: bản rõ: hengapvaothubay

3.2. Mã hóa cổ điển

3.2.2. Mã thay thế đơn giản

- Khoá là một hoán vị h của bảng chữ cái Z
- Mã hóa: mỗi ký hiệu của thông báo được thay thế bằng ảnh của nó qua hoán vị h
- Z_{26} là bảng chữ cái tiếng Anh (gồm 26 kí tự A-Z)
- Có 26! (≈ 4.10^26) hoán vị (khoá)

3.2. Mã hóa cổ điển

3.2.2. Mã thay thế đơn giản

- VD: Mã hóa p="love"

→ bản mã c=bfeh

- Giải mã c="gflh"

→ bản rõ p=hope

Chọn một hoán vị p: $\mathbf{Z}_{26} \rightarrow \mathbf{Z}_{26}$ làm khoá.

VD:

- Mã hoá $e_p(a)=X$

a	b	c	d	e	f	g	h	i	j	k	l	m
X	N	Y	A	H	P	O	G	Z	Q	W	B	T

n	o	p	q	r	s	t	u	v	w	x	y	z
S	F	L	R	C	V	M	U	E	K	J	D	I

- Giải mã $d_p(A)=d$

A	B	C	D	E	F	G	H	I	J	K	L	M
d	l	r	y	v	o	h	e	z	x	w	p	t

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	g	f	j	q	n	m	u	s	k	a	c	i

3.2. Mã hóa cổ điển
3.2.3. Mã dịch vòng (mã Ceasar)

- Plaintext: CRYPTOGRAPHY
- K=5
- Ciphertext: HWDUYTLWFUMD

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

3.2. Mã hóa cổ điển

3.2.3. Mã dịch vòng (mã Ceasar)

- Giả sử $\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_{26}$ với $0 \le k \le 25$, ta định nghĩa:

$$e_k(x) = x + k \bmod 26$$

$$d_k(y) = y - k \bmod 26$$

$$(x, y \in Z_{26})$$

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

3.2. Mã hóa cổ điển

3.2.3. Mã dịch vòng (mã Ceasar)

- Chuyển các ký tự thành số tương ứng A->Z~ 0->25
- Mã hóa $e_k(x)= x+k \bmod 26$
- Giải mã $d_k(y) = y-k \bmod 26$

VD $-3 \bmod 26= -3+26 =23$

$-30 \bmod 26= -30+26+26=22$

3.2. Mã hóa cổ điển

3.2.3. Mã dịch vòng (mã Ceasar)

- VD: mã hóa p=meetmeatsunset, khóa k="c"

c= OGGVOGCVUWPUGV

k=v

P=12.4.4.19.12.4.0.19.18.20.13.18.4.19

C=7.25.25.14.7.25.21.14.13.15.8.13.25.14

C=HZZOHZVONPINZO

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

3.2. Mã hóa cổ điển

3.2.3. Mã dịch vòng (mã Ceasar)

- VD: cho bản mã c=AHFBHSXANH

Khóa k="z". Hãy tìm bản rõ ban đầu

C=0.7.5.1.7.18.23.0.13.7

k=25

$D_k(y) = y-k \bmod 26$

P=1.8.6.2.8.19.24.1.14.8

➔P= BIGCITYBOI

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

3.2. Mã hóa cổ điển

3.2.4. Mã dịch chuyển Vigenere

Khoá: CHIFFRE
Bản rõ: VIGENERE
Bản mã: XPOJSVVG

Mã dịch chuyển – Shift Cypher

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

3.2. Mã hóa cổ điển

3.2.4. Mã dịch chuyển Vigenere

- Khóa k là một chuỗi d ký tự. Khi mã hóa sẽ được viết lặp lại bên dưới thông báo cho đến khi khóa K có độ dài bằng với P, cộng mod 26 lần lượt với từng ký tự của bản rõ.
- Ci=Pi+Ki mod 26
- VD: p= meetmeatsunset

12.4.4.19.12.4.0.19.18.20.13.18.4.19

k= free 5.17.4.4.5.17.4.4.5.17.4.4.5.17

C=17.21.8.23.17.21.4.23.23.11.17.22.9.10

C=RVIXRVEXXLRWJK

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

3.2. Mã hóa cổ điển

3.2.4. Mã dịch chuyển Vigenere

- Khóa k là một chuỗi d ký tự. Khi mã hóa sẽ được viết lặp lại bên dưới thông báo cho đến khi khóa K có độ dài bằng với P, cộng mod 26 lần lượt với từng ký tự của bản rõ.
- Ci=Pi+Ki mod 26
- VD: p= meetmeatsunset

12.4.4.19.12.4.0.19.18.20.13.18.4.19

k= free 5.17.4.4.5.17.4.4.5.17.4.4.5.17

C=17.21.8.23.17.21.4.23.23.11.17.22.9.10

C=RVIXRVEXXLRWJK

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

3.2. Mã hóa cổ điển

3.2.4. Mã dịch chuyển Vigenere

- P = “DAIHOCCONGNGHEGIAOTHONGVANTAI“ người ta thu được bản mã C= “KAVVWJCBBOUGUSOPABHPVNTJIUTNW”.
- Hãy tìm khóa mã hóa đã dùng của hệ mã trên,
- sử dụng khóa tìm được mã hóa xâu “InformationTechnology”?

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

3.2. Mã hóa cổ điển

3.2.4. Mã dịch chuyển Vigenere

- P=3.0.8.7.14.2.2.14.13.6.13.6.7.4.6.8.0.14.19.7.14.13.6.21.0.13.19.0.8
- C=10.0.21.21.22.9.2.1.1.14.20.6.20.18.14.15.0.1.7.15.21.13.19.9.8.20.19.13.22
- Ci=Pi+Ki mod 26 →Ki=Ci-Pi mod 26
- Ki=7.0.13.14.8.7.0.13.14.8.7.0.13.14.8.7.0.13.14.8.7.0.13.14.8.7.0.13.14
- Kết luận: k= 7.0.13.14.8 → HANOI

Mã hóa: P=InformationTechnology

- P=8.13.5.14.17.12.0.19.8.14.13.19.4.2.7.13.14.11.14.6.24
- Ki=7.0.13.14.8.7.0.13.14.8.7.0.13.14.8.7.0.13.14.8.7
- Ci=Pi+Ki mod 26
- C= 15.13.18.2.25.19.0.6.22.22.20.19.17.16.15.20.14.24.2.14.5
- Kết luận: C= PNSCZTAGWWUTRQPUOYCOF

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

3.2. Mã hóa cổ điển

3.2.5. Mã Hill

Giải thuật mã hóa:

- Chọn ma trận vuông Hill cấp m (ma trận H) làm khoá.
  - Chia bản rõ thành các khối m ký tự, tạo thành vector P
- •Nhân P với ma trận khóa H để thu được m ký tự tương ứng trong bản mã.
  - C = PH mod 26
  - P = CH^{-1} mod 26

3.2. Mã hóa cổ điển

3.2.5. Mã Hill

Cho $A = \begin{bmatrix} 12 & 5 \\ 3 & 7 \end{bmatrix}$ hãy thực hiện mã hóa và giải mã với xâu S = “HARD”.

Có 12*7 -3*5 #0 → A có thể làm khóa

Mã hóa: HA và RD

p1=HA → (7,0)

c1= $(7,0)\begin{bmatrix} 12 & 5 \\ 3 & 7 \end{bmatrix}$=(7*12+3*0, 7*5+0*7) =(84,35) mod 26=(6,9)

→GJ

P2=RD → (17,3) → (213,106) mod 26 =(5,2)

c2= FC

→ Bản mã c= GJFC

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

3.2. Mã hóa cổ điển

3.2.6. Mã Hill

Cho hệ mã Hill có M=3 (khóa là ma trận vuông cấp 3) và bảng chữ cái là Tiếng Anh, cho khóa K là ma trận sau:

1	3	5
6	4	9
3	5	7

Hãy mã hóa xâu P = ”INFORMATION”?

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

3.2. Mã hóa cổ điển

3.2.6. Mã Hill

8 13 5

101 mod 26 =23

101 mod 26 =23

192 mod 26 =10

14 17 12

152 mod 26 =22

170 mod 26 =14

307 mod 26 =21

0 19 8

138 mod 26 =8

116 mod 26 =12

227 mod 26 =19

14 13 0

92 mod 26 =14

94 mod 26 =16

187 mod 26 =5

XXKWOVIMTOQ

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

3.2. Mã hóa cổ điển

3.2.6. Mã Hill

Cho hệ mã Hill có M=3 (khóa là ma trận vuông cấp 3) và bảng chữ cái là Tiếng Anh, cho khóa K là ma trận sau:

1	5	8
4	2	3
5	6	7

Hãy mã hóa xâu P = ”INFORMATION”?

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

3.2. Mã hóa cổ điển

3.2.6. Mã Hill

INF →(8 13 5)

(8*1+13*4+5*5,
8*5+13*2+5*6,
8*8+13*3+5*7)

=(85,96,138) mod 26

=(7,18,8)→HSI

ORM →14 17 12

142 mod 26 =12

176 mod 26 =20

247 mod 26 =13

ATI → 0 19 8

116 mod 26 =12

86 mod 26 =8

113 mod 26 =9

ONA → 14 13 0

66 mod 26 =14

96 mod 26 =18

151 mod 26 =21

HSIMUNMIJOS

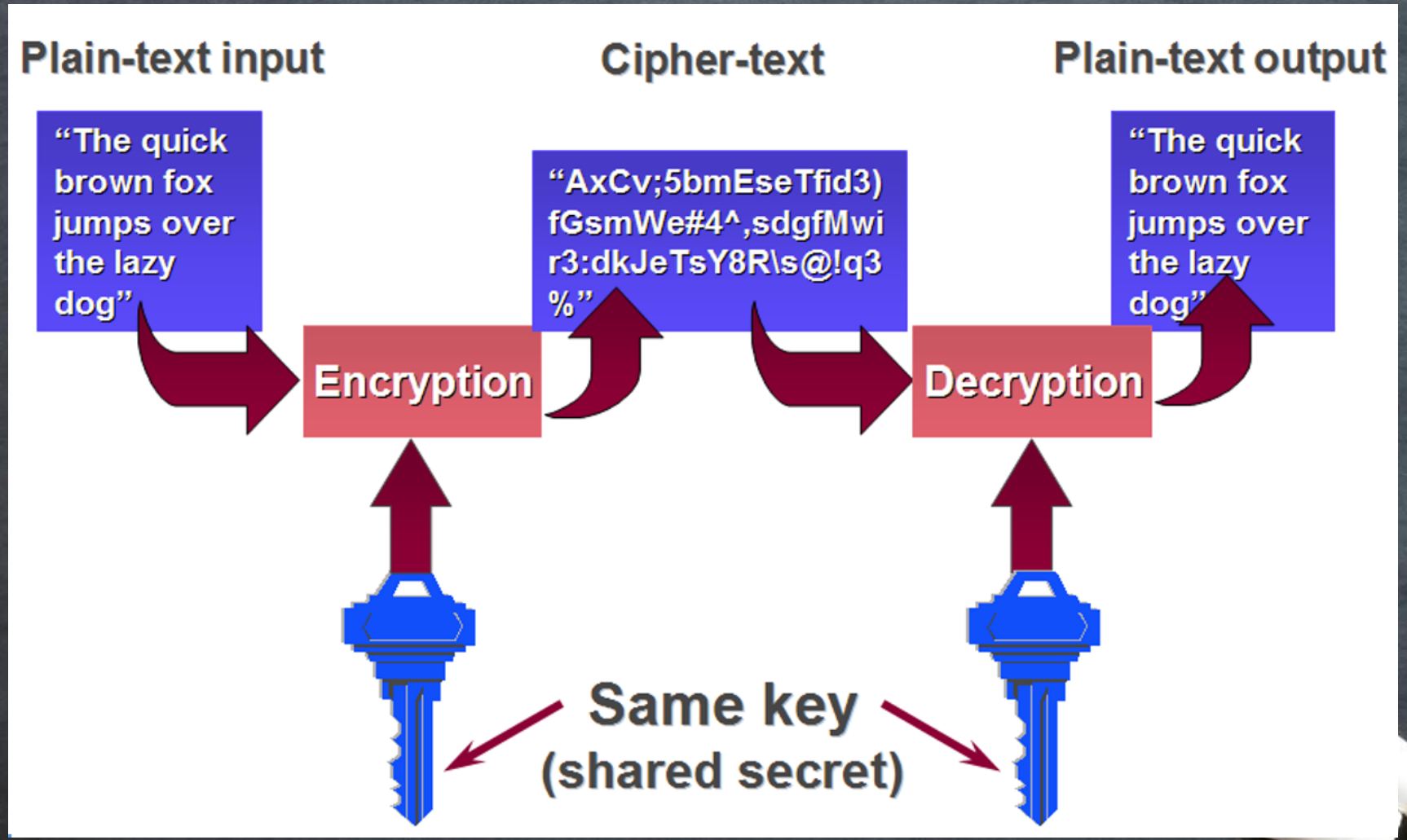
1	5	8
4	2	3
5	6	7

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

3.3. Các hệ mã hóa khóa đối xứng

- Các giải thuật mã hóa khóa đối xứng (symetric key encryption)
  - Còn gọi là mã hóa khóa riêng hay bí mật (secret/private key encryption):
  - Sử dụng một khóa (key) duy nhất cho cả quá trình mã hóa và giải mã.
- Đặc điểm:
  - Kích thước khóa tương đối ngắn (64, 128, 192, 256 bít)
  - Tốc độ nhanh
  - Độ an toàn cao
  - Khó khăn trong quản lý và phân phối khóa.

3.3. Các hệ mã hóa khóa đối xứng



3.3. Các hệ mã hóa khóa đối xứng

3.3.1. DES

- DES (Data Encryption Standard) được sử dụng phổ biến:
  - DES được phát triển tại IBM vào đầu những năm 1970;
  - Được thừa nhận là chuẩn mã hóa tại Mỹ (NSA) vào năm 1976;
  - DES được sử dụng rộng rãi trong những năm 70 và 80.
- Hiện nay DES không được coi là an toàn do:
  - Không gian khóa nhỏ (khóa 64 bít, trong đó thực sử dụng 56 bít)
  - Tốc độ tính toán của các hệ thống máy tính ngày càng nhanh.
- Đặc điểm:
  - Là dạng mã hóa khối, kích thước khối vào 64 bít
  - Khóa 64 bít, trong đó thực sử dụng 56 bít, 8 bít dùng cho kiểm tra chẵn lẻ
  - DES sử dụng chung một giải thuật cho mã hóa và giải mã.

3.3. Các hệ mã hóa khóa đối xứng

3.3.1. DES

- Các bước thực hiện mã hóa của DES với mỗi khối dữ liệu 64 bít:
  - Bước hoán vị khởi tạo (IP – Initial Permutation);
  - 16 vòng lặp chính thực hiện xáo trộn dữ liệu theo hàm Feistel (F);
  - Bước hoán vị nghịch đảo/kết thúc (FP – Final Permutation).
- Sử dụng phép $\oplus$ (XOR) để kết hợp trong quá trình lặp.

A	0	0	1	1
B	0	1	0	1
A $\oplus$ B	0	1	1	0

3.3. Các hệ mã hóa khóa đối xứng

3.3.1. DES

- Bước 1: Hoán vị khởi tạo

  $x_0 = IP(x) = L_0R_0$

- Bước 2: tính L_iR_i, $1 \leq i \leq 16$ theo quy tắc sau:

  $L_i = R_{i-1}$

  $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

- Bước 3: Hoán vị nghịch đảo

  $y = IP^{-1}(R_{16}L_{16})$

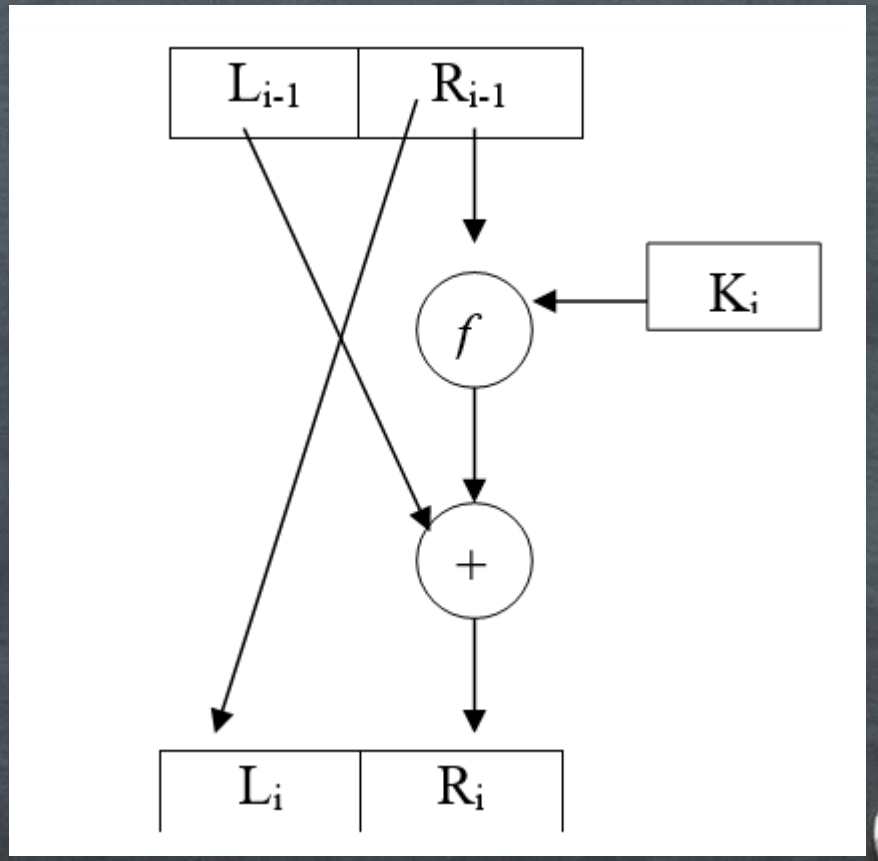
3.3. Các hệ mã hóa khóa đối xứng

3.3.1. DES

Một vòng của DES:

$L_i = R_{i-1}$

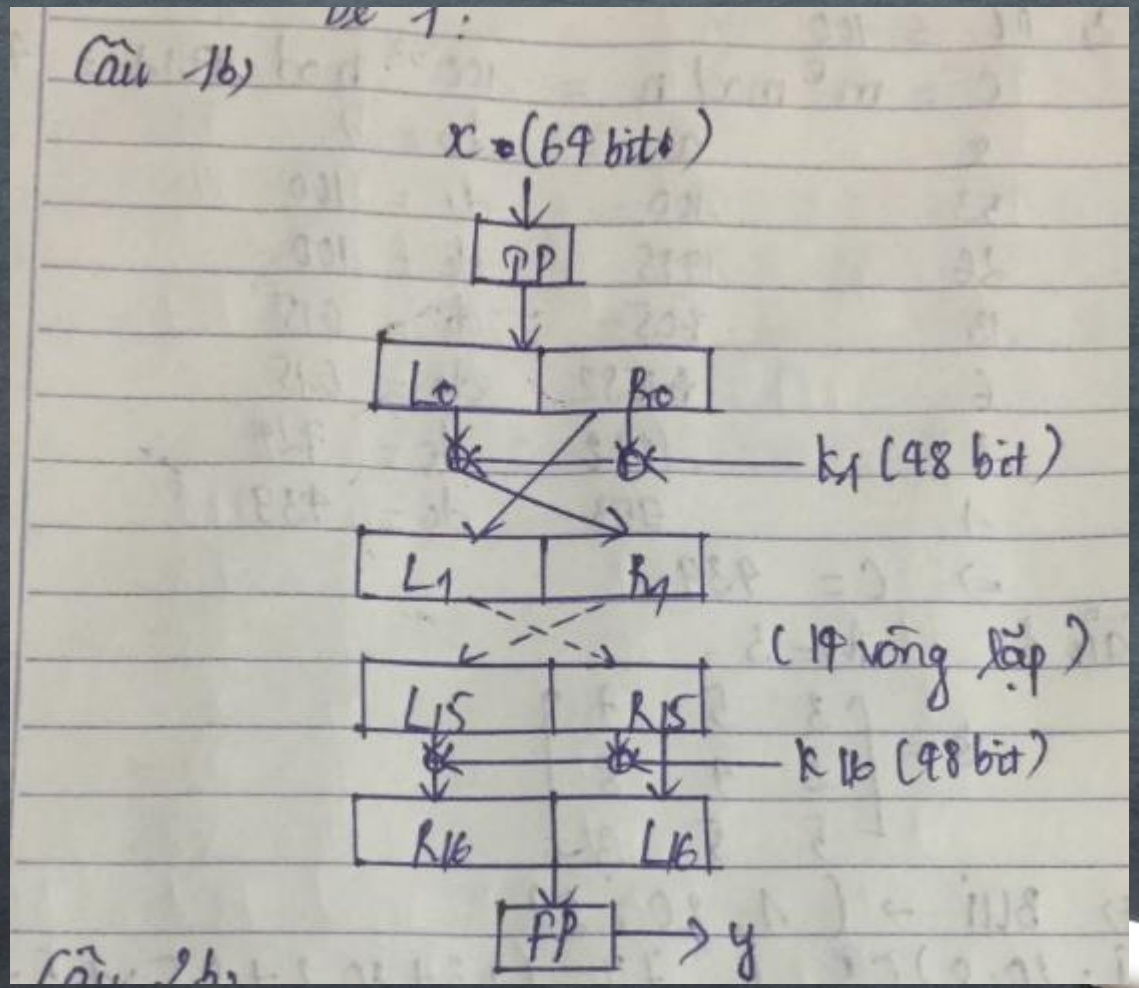
$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$



3.3. Các hệ mã hóa khóa đối xứng

3.3.1. DES

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	31	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7



IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

3.3. Các hệ mã hóa khóa đối xứng

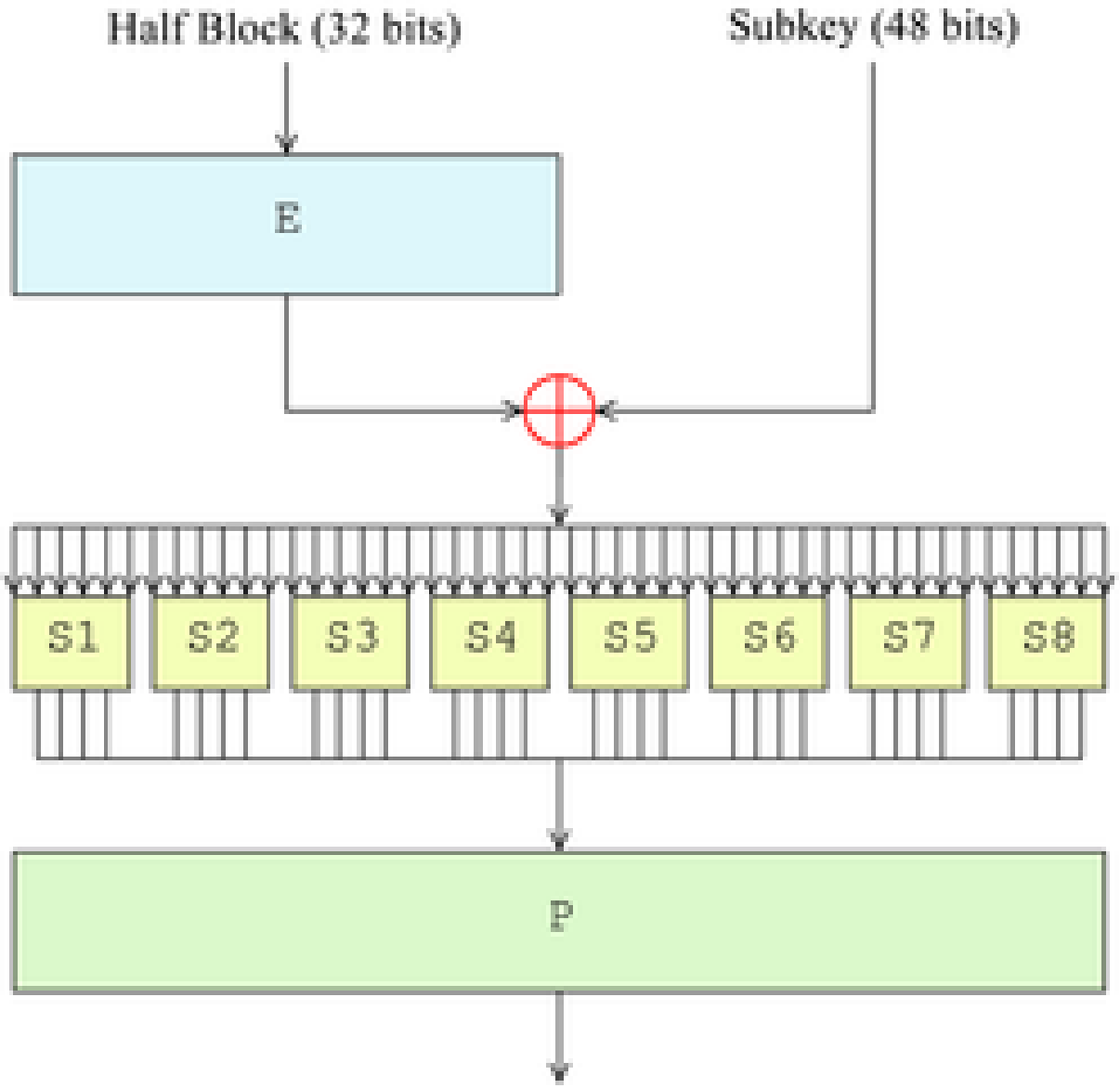
3.3.1. DES

- Các bước thực hiện hàm F (Fiestel) của DES:

  $f(R_{i-1},K_i)$

- E (Expansion) – mở rộng
- ⊕: trộn với một phần khóa
- S_i (Substitution) - thay thế
- P – Hoán vị.

Bảng chọn E bít					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1



3.3. Các hệ mã hóa khóa đối xứng

3.3.1. DES

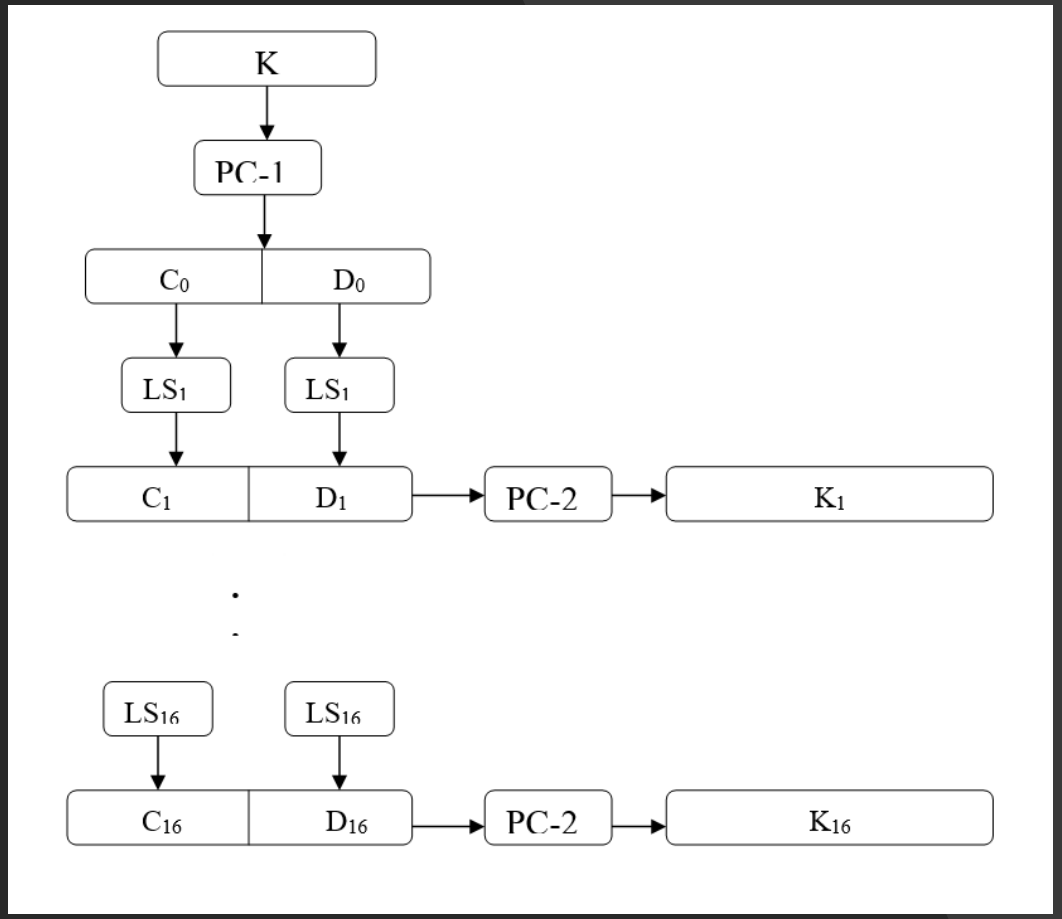
Các bước thực hiện hàm F (Fiestel) với khối dữ liệu 32 bít của DES:

- E (Expansion): thực hiện mở rộng 32 bít đầu vào thành 48 bít bằng cách nhân đôi một nửa số bit.
- ⊕: Trộn 48 bit ở bước E với khóa phụ 48 bít. Có 16 khóa phụ được tạo từ khóa chính để sử dụng cho 16 vòng lặp.
- S_i (Substitution): Khối dữ liệu 48 bit được chia thành 8 khối 6 bít và được chuyển cho các bộ thay thế (S1-S8).
  - Mỗi bộ thay thế sử dụng phép chuyển đổi phi tuyến tính để chuyển 6 bit đầu vào thành 4 bit đầu ra theo bảng tham chiếu. Các bộ thay thế là thành phần nhân an ninh (security core) của DES.
- P: 32 bít đầu ra từ các bộ thay thế được sắp xếp bằng phép hoán vị cố định (fixed permutation) cho ra đầu ra 32 bít.

3.3. Các hệ mã hóa khóa đối xứng

3.3.1. DES

- Tạo bộ khóa phụ cho 16 vòng lặp:
  - 56 bít khóa được chọn từ khóa 64 bit ban đầu bởi PC-1 (Permuted Choice 1). 8 bit còn lại được hủy hoặc dùng để kiểm tra chẵn lẻ;
  - 56 bít được chia thành 2 phần 28 bit, mỗi phần được xử lý riêng;
  - Mỗi phần được quay trái 1 hoặc 2 bit.
  - Hai phần được ghép lại và 48 bit được chọn làm khóa phụ 1 bởi PC-2;
  - Lặp lại bước trên để tạo 15 khóa phụ còn lại.



3.3. Các hệ mã hóa khóa đối xứng

3.3.1. DES

PC-1	PC-2

56	48	40	32	24	16	8
0	57	49	41	33	25	17
9	1	58	50	42	34	26
18	10	2	59	51	43	35
62	54	46	38	30	22	14
6	61	53	45	37	29	21
13	5	60	52	44	36	28
20	12	4	27	19	11	3

56 bít

13	16	10	23	0	4	2	27
14	5	20	9	22	18	11	3
25	7	15	6	26	19	12	1
40	51	30	36	46	54	29	39
50	44	32	47	43	48	38	55
33	52	45	41	49	35	28	31

48 bít

3.3. Các hệ mã hóa khóa đối xứng

3.3.1. DES

- Giải mã trong DES:
  - Có thể sử dụng giải thuật mã hóa DES để giải mã;
  - Các bước thực hiện giống quá trình mã hóa;
  - Các khóa phụ sử dụng cho các vòng lặp được sử dụng theo trật tự ngược lại: Khóa phụ 16, 15,…, 2, 1 cho các vòng 1, 2,…, 15, 16 tương ứng.

3.3. Các hệ mã hóa khóa đối xứng

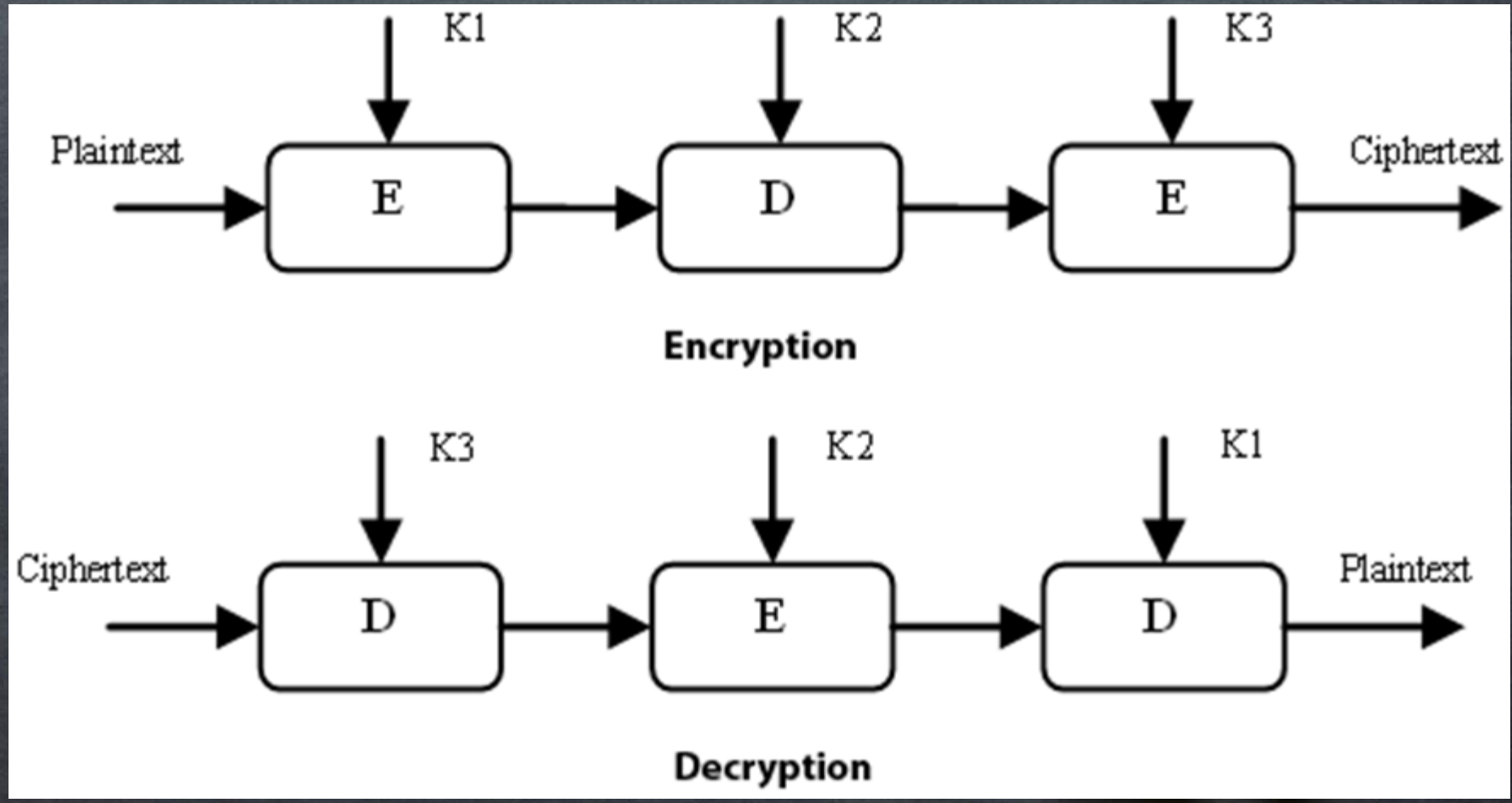
3.3.1. DES

- Triple DES (3-DES) còn được gọi là Triple Data Encryption Algorithm (TDEA hoặc Triple DEA) được phát triển từ DES bằng cách áp dụng DES 3 lần cho mỗi khối dữ liệu;
- Triple DES sử dụng bộ 3 khóa DES: K1, K2, K3, mỗi khóa kích thước hiệu dụng 56 bít;
- Các lựa chọn bộ khóa:
  - Lựa chọn 1: cả 3 khóa độc lập (168 bít)
  - Lựa chọn 2: K1 và K2 độc lập, K3 = K1 (112 bít)
  - Lựa chọn 3: 3 khóa giống nhau, K1 = K2 = K3 (56 bít).
- Kích thước khối dữ liệu vào: 64 bít.

3.3. Các hệ mã hóa khóa đối xứng

3.3.1. DES

- Triple DES



3.3. Các hệ mã hóa khóa đối xứng

3.3.1. DES

- **Triple DES**
  - Giải thuật mã hóa:
    - ciphertext = $E_{K3}(D_{K2}(E_{K1}(plaintext)))$

    → Mã hóa bằng khóa K1, giải mã bằng K2 và mã hóa bằng K3.
  - Giải thuật giải mã:
    - plaintext = $D_{K1}(E_{K2}(D_{K3}(ciphertext)))$

    → Giải mã bằng K3, mã hóa bằng K2 và giải mã bằng K1.

3.3. Các hệ mã hóa khóa đối xứng

3.3.2. AES

- AES (Advanced Encryption Standard) là một chuẩn mã hóa dữ liệu được NIST công nhận năm 2001;
- AES được xây dựng dựa trên Rijndael cipher phát triển bởi 2 nhà mật mã học người Bỉ là Joan Daemen và Vincent Rijmen;
- Kích thước khối dữ liệu của AES là 128 bít;
- Kích thước khóa có thể là 128, 192, hoặc 256 bit (là bội của 32 và lớn nhất là 256 bít);
- AES được thiết kế dựa trên mạng hoán vị-thay thế (substitution-permutation network);
  - Có thể đạt tốc độ cao trên cả cài đặt phần mềm và phần cứng.

3.3. Các hệ mã hóa khóa đối xứng

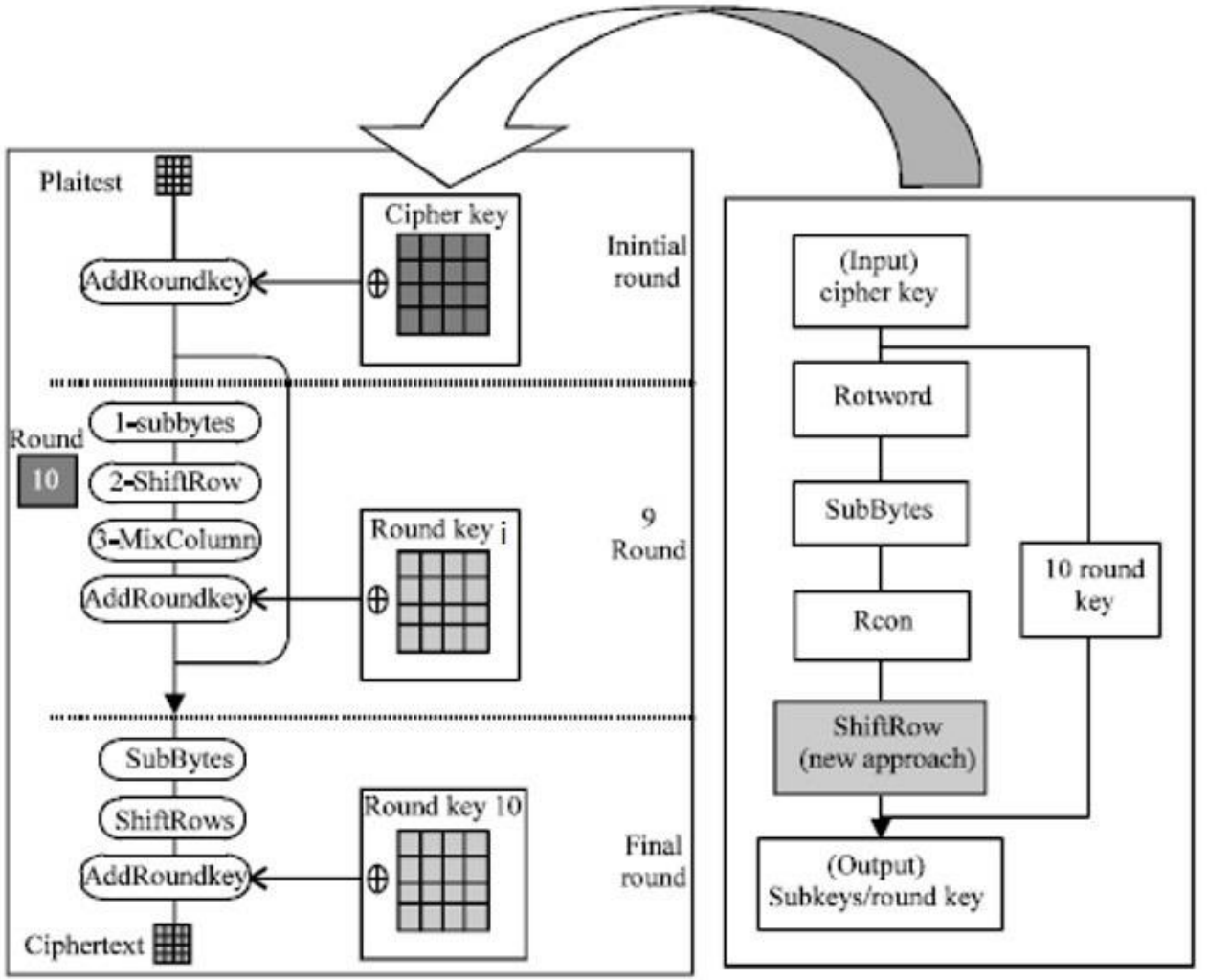
3.3.2. AES

- AES vận hành dựa trên một ma trận 4x4, được gọi là *state* (trạng thái);
- Kích thước của khóa quyết định số vòng lặp chuyển đổi cần thực hiện để chuyển bản rõ thành bản mã:
  - 10 vòng lặp với khóa 128 bít;
  - 12 vòng lặp với khóa 192 bít;
  - 14 vòng lặp với khóa 256 bít.

3.3. Các hệ mã hóa khóa đối xứng

3.3.2. AES

- Các bước xử lý chính của AES với khóa 128 bít



3.3. Các hệ mã hóa khóa đối xứng

3.3.2. AES

- Mô tả khái quát giải thuật AES:
  1. Mở rộng khóa (KeyExpansion): các khóa phụ dùng trong các vòng lặp được sinh ra từ khóa chính AES sử dụng thủ tục sinh khóa Rijndael.
  2. Vòng khởi tạo (InitialRound)
     a) AddRoundKey: Mỗi byte trong *state* được kết hợp với khóa phụ sử dụng XOR

3.3. Các hệ mã hóa khóa đối xứng

3.3.2. AES

- Mô tả khái quát giải thuật AES:

3. Các vòng lặp chính (Rounds)
   a) SubBytes: bước thay thế phi tuyến tính, trong đó mỗi byte trong *state* được thay thế bằng một byte khác sử dụng bảng tham chiếu;
   b) ShiftRows: bước đổi chỗ, trong đó mỗi dòng trong *state* được dịch một số bước theo chu kỳ;
   c) MixColumns: trộn các cột trong *state*, kết hợp 4 bytes trong mỗi cột.
   d) AddRoundKey.
4. Vòng cuối (Final Round - không MixColumns)
   a) SubBytes;
   b) ShiftRows;
   c) AddRoundKey.

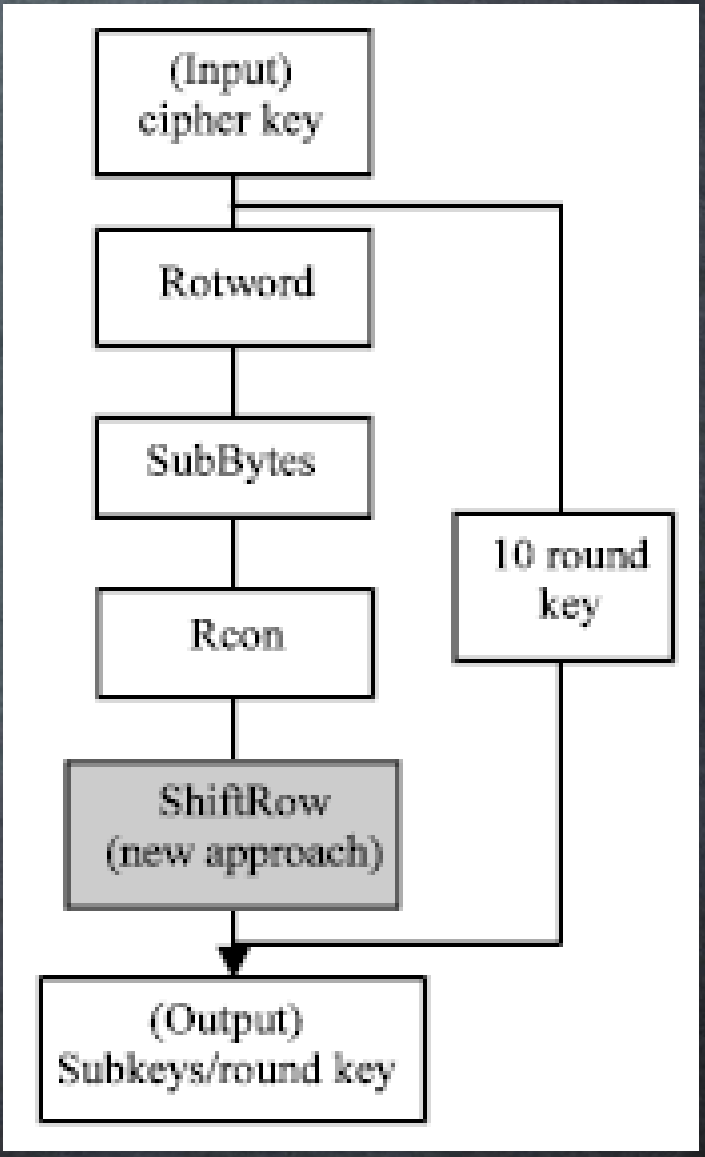
3.3. Các hệ mã hóa khóa đối xứng

3.3.2. AES

- Mở rộng khóa sử dụng thủ tục sinh khóa Rijndael:
  - Rotword: quay trái 8 bít;
  - SubBytes
  - Rcon: tính toán giá trị Rcon(i)

$$\text{rcon}(i) = x^{(i-1)} \mod x^8 + x^4 + x^3 + x + 1$$

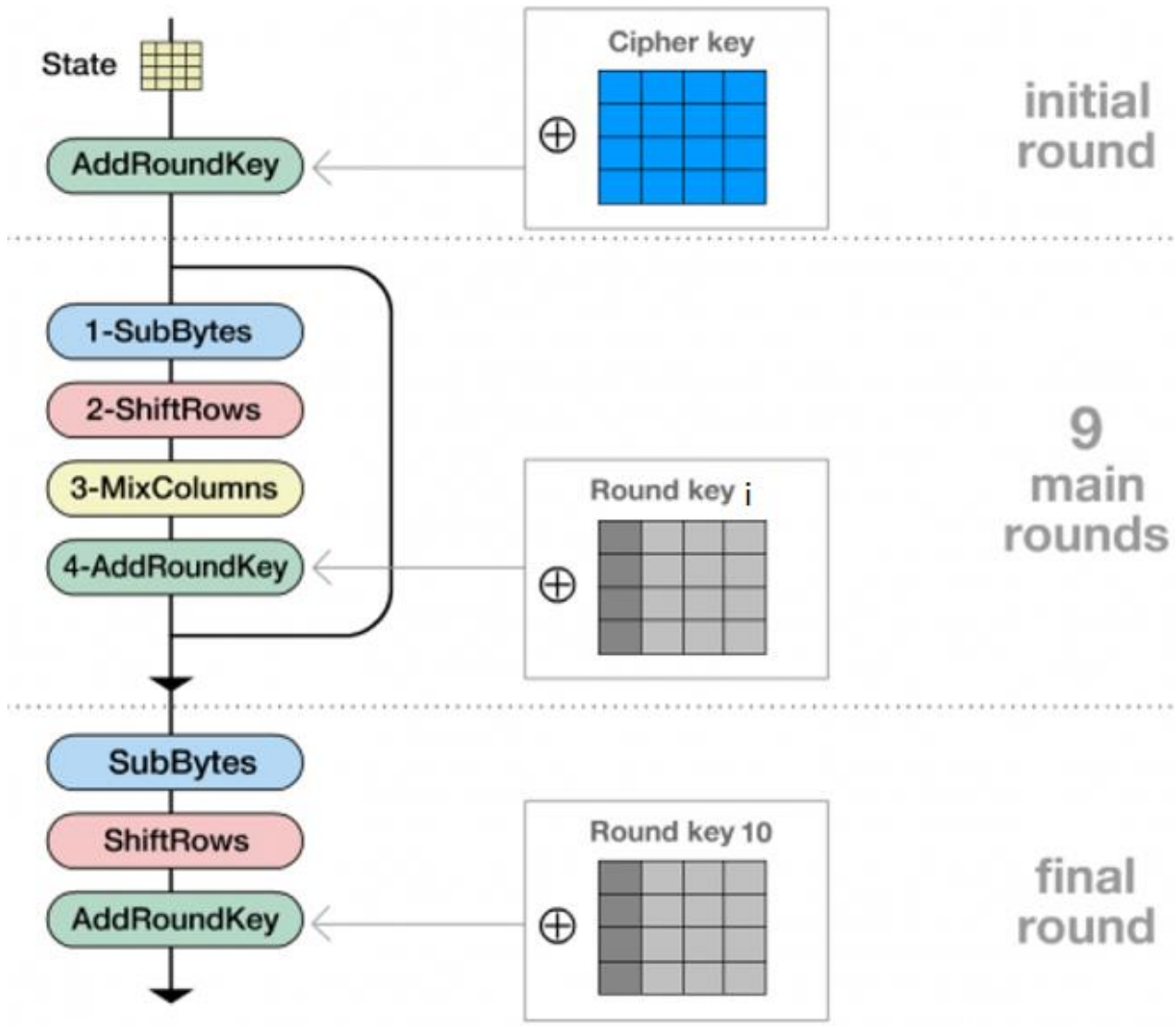
  - ShiftRow



3.3. Các hệ mã hóa khóa đối xứng

3.3.2. AES

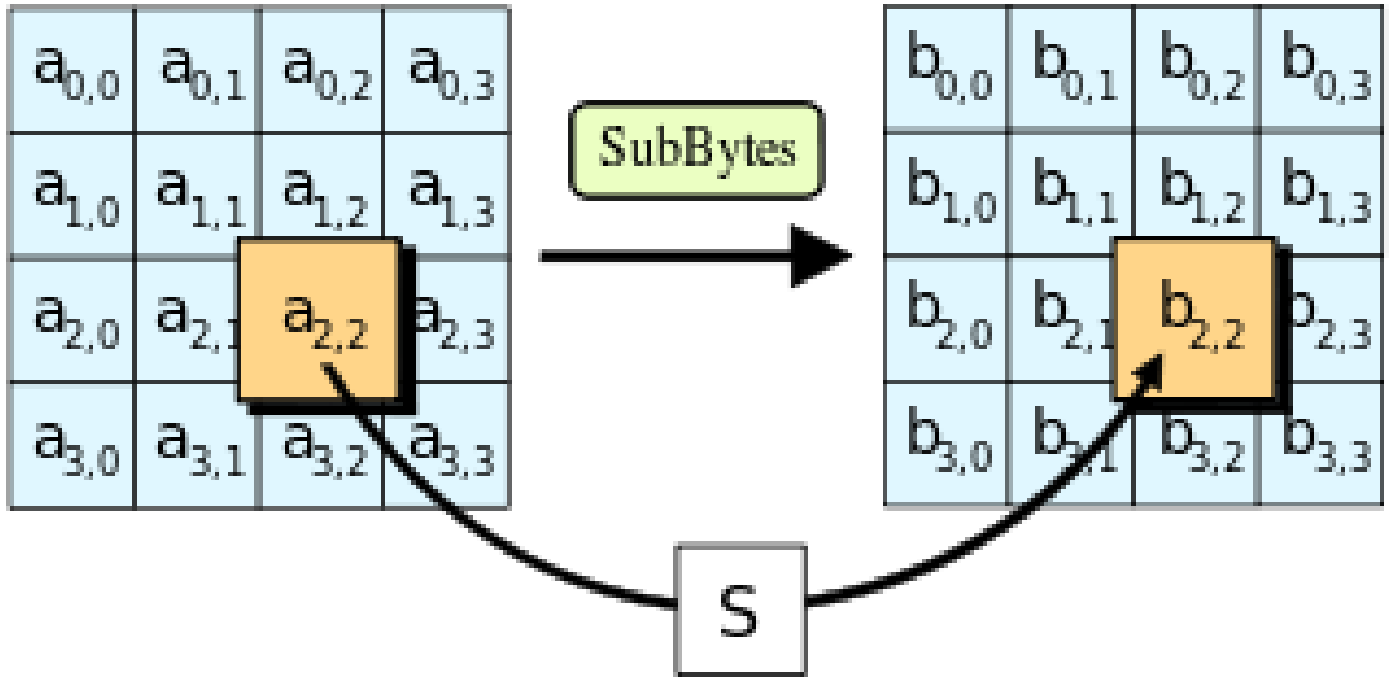
- Các bước xử lý chính của AES với khóa 128 bít



3.3. Các hệ mã hóa khóa đối xứng

3.3.2. AES

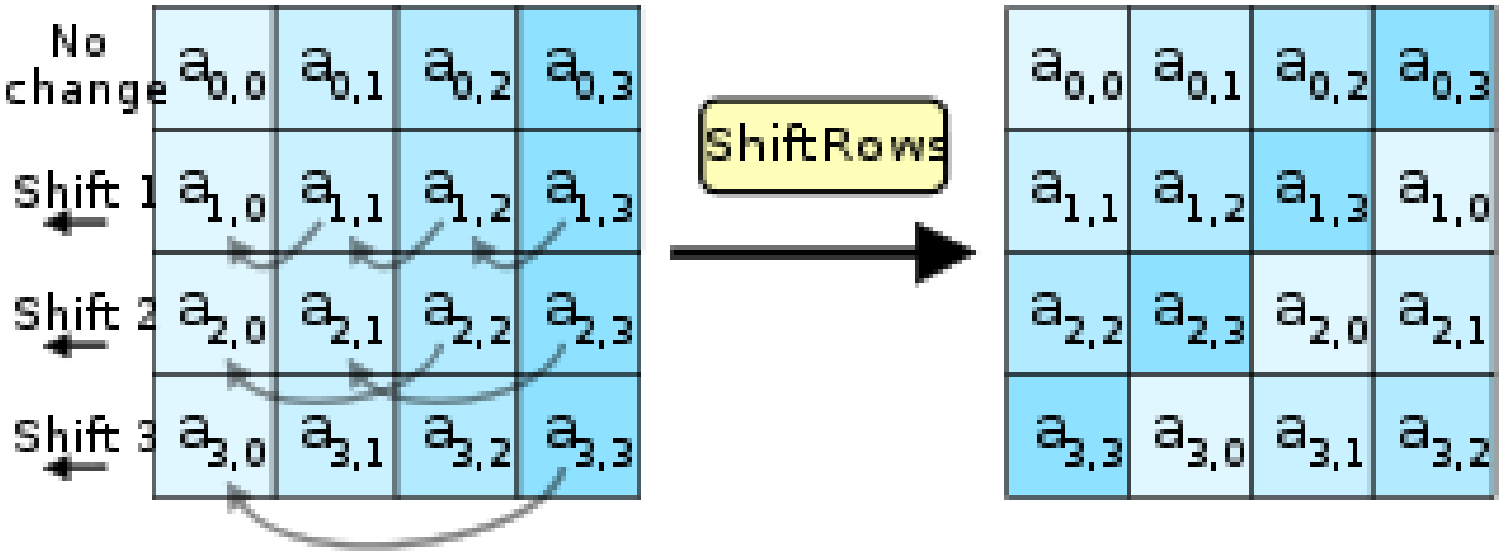
- Bước SubBytes:
  - Mỗi byte trong ma trận state được thay thế bởi 1 byte trong Rijndael S-box, hay $b_{ij} = S(a_{ij})$



3.3. Các hệ mã hóa khóa đối xứng

3.3.2. AES

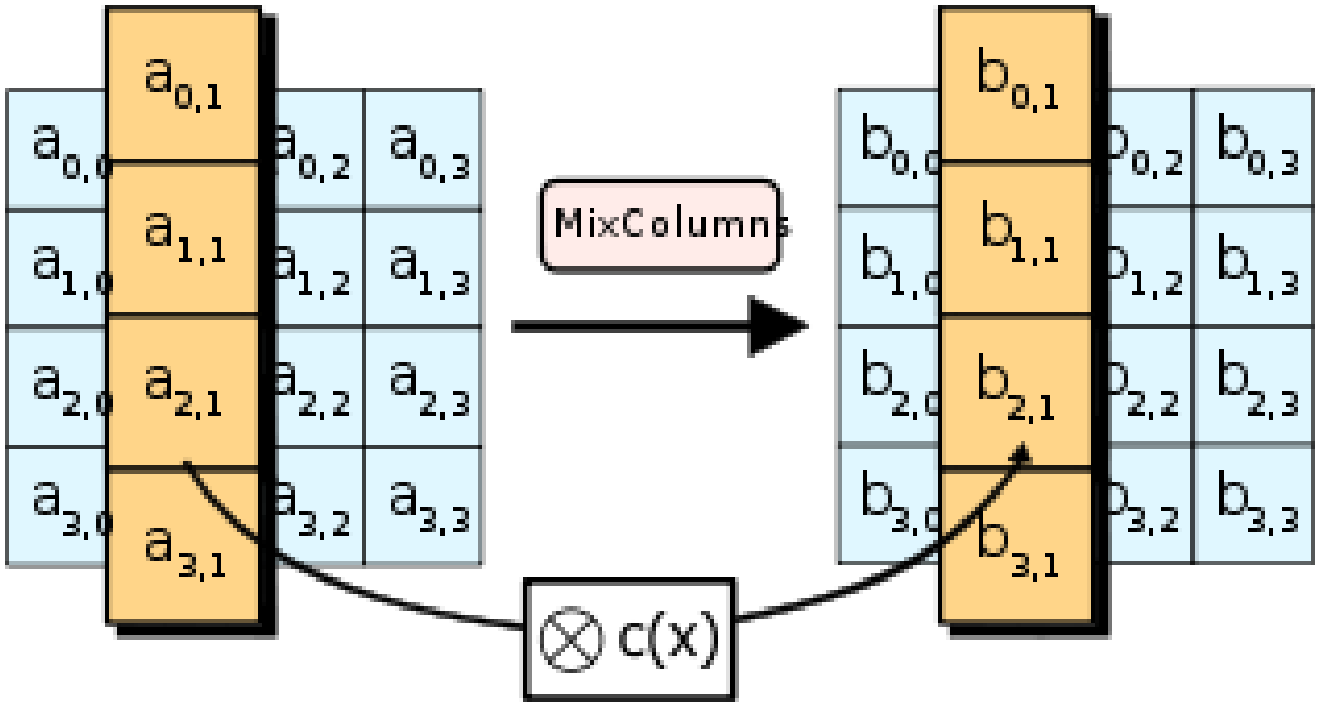
- Bước ShiftRows:
  - Các dòng của ma trận state được dịch theo chu kỳ sang trái;
  - Dòng thứ nhất giữ nguyên.



3.3. Các hệ mã hóa khóa đối xứng

3.3.2. AES

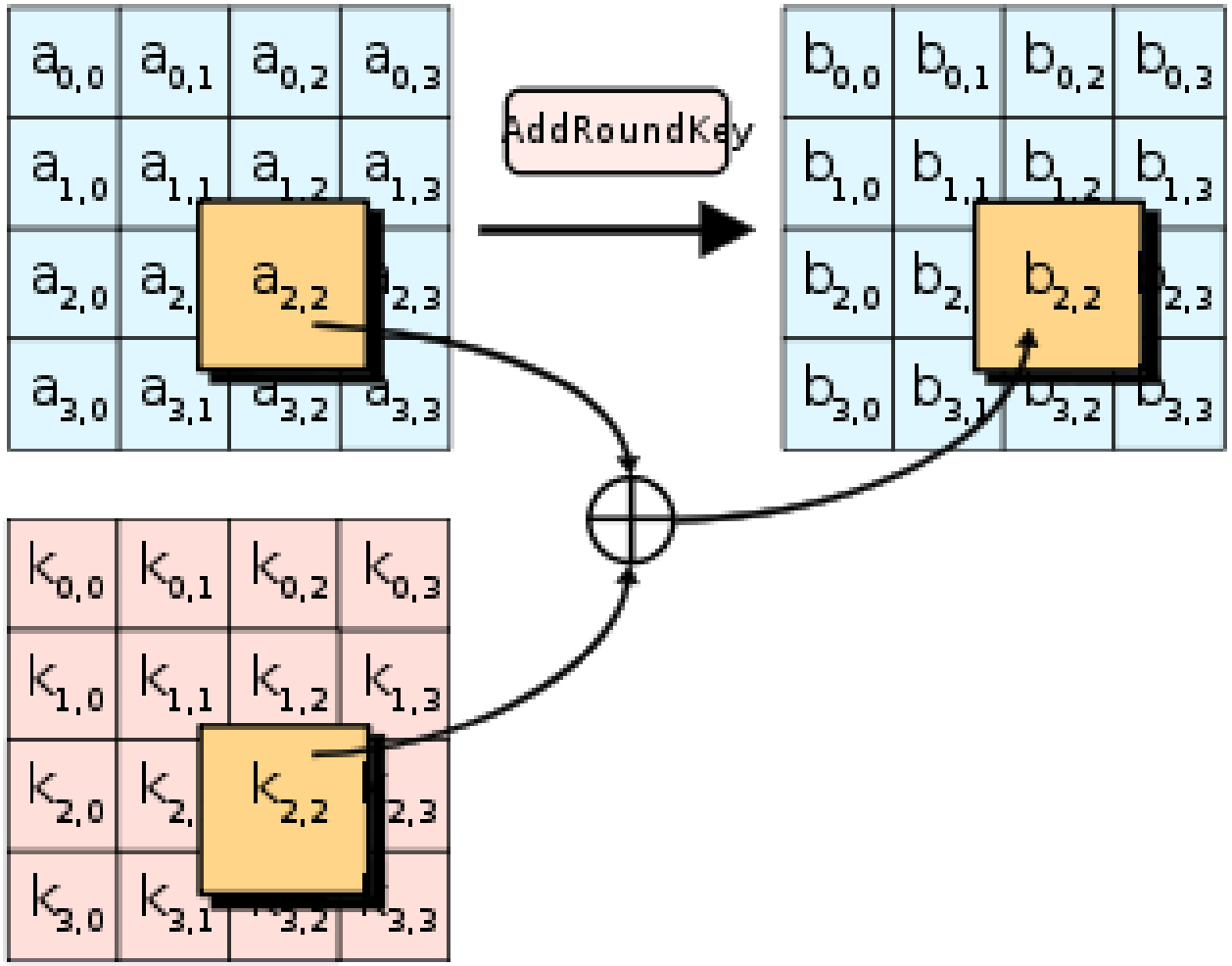
- Bước MixColumns:
  - Mỗi cột của ma trận state được nhân với một đa thức c(x)=3x^3+x^2+x+2



3.3. Các hệ mã hóa khóa đối xứng

3.3.2. AES

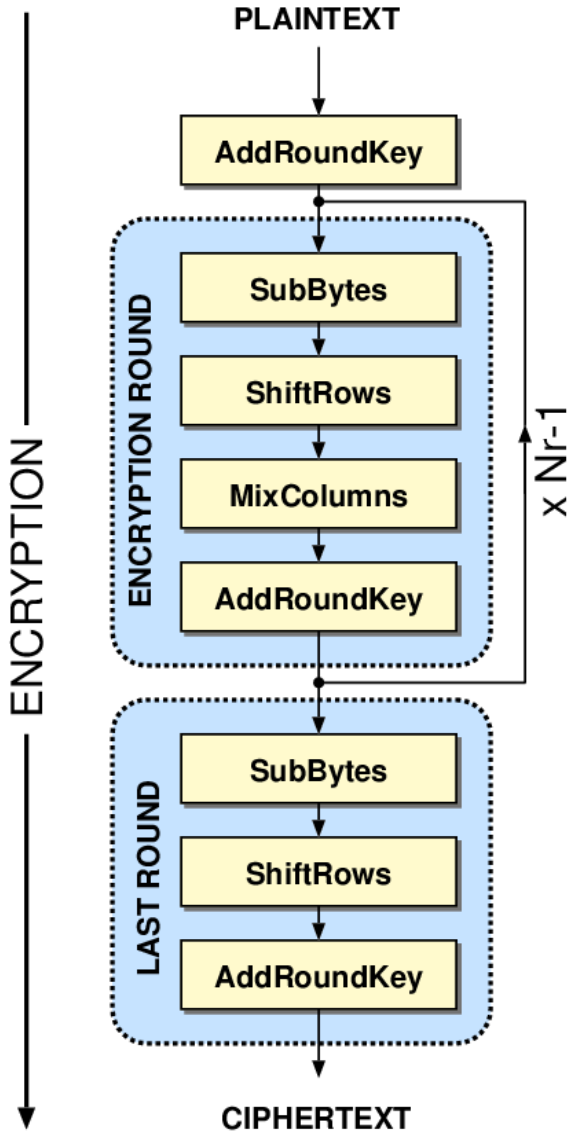
- Bước AddRoundKey:
  - Mỗi byte của ma trận state được kết hợp với một byte của khóa phụ sử dụng phép ⊕ (XOR).

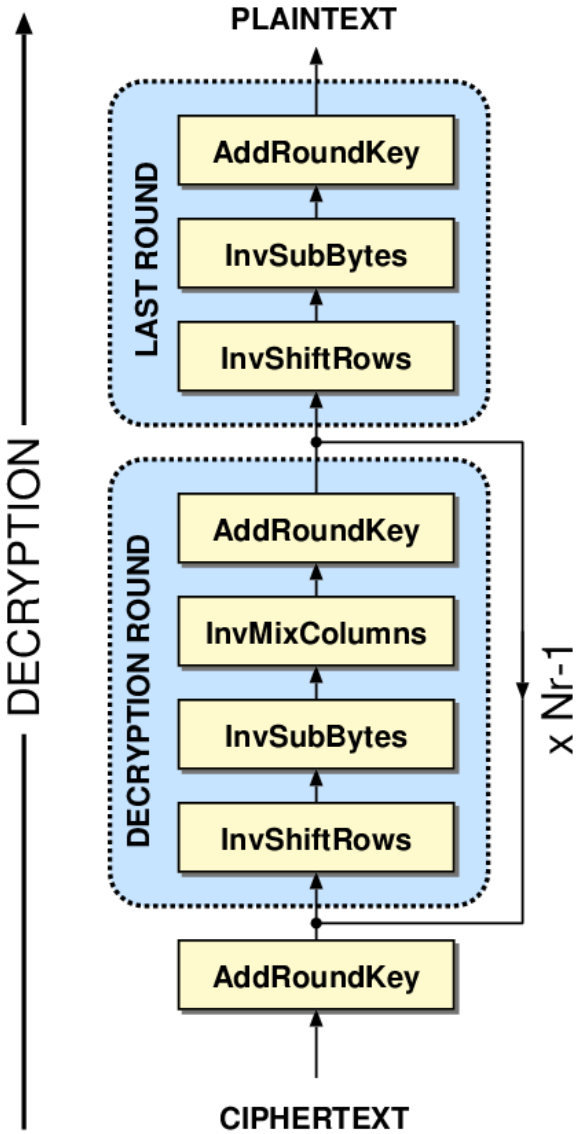


3.3. Các hệ mã hóa khóa đối xứng

3.3.2. AES

- Quá trình mã hóa và giải mã của AES

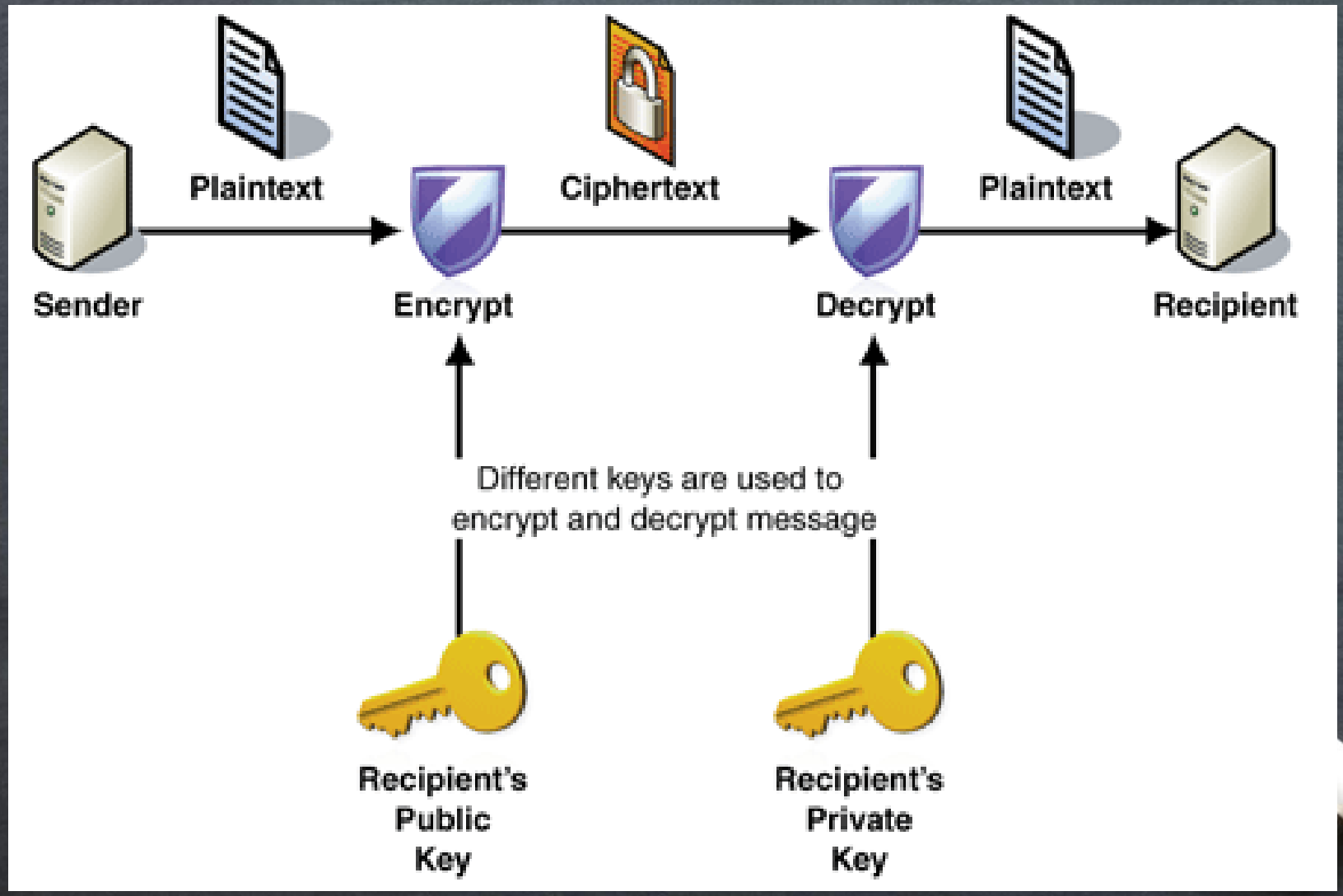




3.4. Các hệ mã hóa khóa bất đối xứng

- Các giải thuật mã hóa khóa bất đối xứng (asymetric key encryption)
  - Còn gọi là mã hóa khóa công khai (public key encryption):
  - Sử dụng một cặp khóa (key pair): một khóa cho mã hóa và một khóa cho giải mã.
- Đặc điểm:
  - Kích thước khóa lớn (1024 – 3072 bít)
  - Tốc độ chậm
  - Độ an toàn cao
  - Thuận lợi trong quản lý và phân phối khóa.

3.3. Các hệ mã hóa khóa bất đối xứng



3.4. Các hệ mã hóa khóa bất đối xứng

- Các giải thuật mã hóa khóa bất đối xứng điển hình:
  - RSA
  - ElGamal
  - Rabin
  - McEliece
  - Knapsack

3.4. Các hệ mã hóa khóa bất đối xứng

3.4.1. RSA

- Giải thuật mã hóa RSA được 3 nhà khoa học Ronald Rivest, Adi Shamir và Leonard Adleman phát minh năm 1977;
- Độ an toàn của RSA dựa trên tính khó của việc phân tích số nguyên rất lớn (số có hàng trăm chữ số thập phân);
- RSA sử dụng một cặp khóa:
  - Khóa công khai (Public key) dùng để mã hóa *(Kp của người nhận)*
  - Khóa riêng (Private key) dùng để giải mã *(Ks của người nhận)*
  - Chỉ khóa riêng cần giữ bí mật. Khóa công khai có thể công bố rộng rãi.
- Kích thước khóa của RSA:
  - Khóa < 1024 bít không an toàn hiện nay.
  - Khuyến nghị dùng khóa >= 2048 bít. Tương lai nên dùng khóa 3072 bít.

3.4. Các hệ mã hóa khóa bất đối xứng

3.4.1. RSA

- Thủ tục sinh khóa RSA:
  - Tạo 2 số nguyên tố lớn p và q;
  - Tính n = p x q
  - Tính $\Phi(n) = (p-1) \times (q-1)$
  - Chọn số e sao cho $0 < e < \Phi(n)$ và UCLN(e, $\Phi(n)$) = 1
  - Chọn số d sao cho $d \equiv e^{-1} \bmod \Phi(n)$,

    hoặc $(d \times e) \bmod \Phi(n) = 1$

    (d là molulo nghịch đảo của e mod $\Phi(n)$
- Ta có (n, e) là khóa công khai, (n, d) là khóa riêng.

Hàm Ơ-le

- $\Phi(n)$ được gọi là hàm Ơ-le của n
- Hàm Ơ-le của n được tính bằng số các số nhỏ hơn n và nguyên tố cùng nhau với n
- VD1: n=6, tập hợp các số nhỏ hơn 6 {0,1,2,3,4,5}

  Các số nhỏ hơn 6 và nguyên tố cùng nhau với 6 {1,5}

  → $\Phi(6)=2$
- VD2: n=5 → $\Phi(5) =4 =5-1$
- Nếu p là số nguyên tố thì $\Phi(p)=p-1$
- Nếu UCLN(p,q)=1 thì $\Phi(p.q)= \Phi(p). \Phi(q)$

3.4. Các hệ mã hóa khóa bất đối xứng

3.4.1. RSA

- Thủ tục mã hóa RSA:
  - Thông điệp m đã được chuyển thành số, m<n
  - Bản mã $c = m^e \bmod n$
- Thủ tục giải mã RSA:
  - Bản mã c, c<n
  - Bản rõ $m = c^d \bmod n$

3.4. Các hệ mã hóa khóa bất đối xứng

3.4.1. RSA

- Ví dụ:
  - Chọn 2 số nguyên tố p=61 và q=53
  - Tính n = p x q = 61 x 53 = 3233
  - Tính $\Phi(n) = (p-1) \times (q-1) = 60 \times 52 = 3120$
  - Chọn số e sao cho 0 < e < 3120 và e và $\Phi(n)$ là số nguyên tố cùng nhau ($\Phi(n)$ không chia hết cho e). Chọn e = 17
  - Tính d thoản mãn $(d*e) \bmod \Phi(n) = 1 \rightarrow (d*17) \bmod 3120 = 1$

    $d = (3120*k + 1)/17$

    → d = 2753 (k=15)
  - Khóa công khai (3233, 17)
  - Khóa bí mật (3233, 2753)

3.4. Các hệ mã hóa khóa bất đối xứng

3.4.1. RSA

- Ví dụ:
  - Mã hóa:
    - Với m = 65,
    - $c = m^e \bmod n = 65^{17} \bmod 3233$

    $=(65^4)^4 * 65 \bmod 3233 = 2790$

    Tính $65^4 \bmod 3233 = 1232$; $1232^4 \bmod 3233 = 789$; $789 * 65 \bmod 3233 = 2790$

    → c = 2790
  - Giải mã:
    - $m = c^d \bmod n = 2790^{2753} \bmod 3233$

    → m = 65

Tính modulo nghịch đảo

Tính $\mathbf{n^{-1} \bmod m}$

- Điều kiện: UCLN(n, m) =1
- n=1 thì $n^{-1} \bmod m = 1$
- Điều kiện dừng: $x_i=1$, kết quả lấy b_i nếu $b_i>0$

Nếu $b_i<0$ thì lấy b_i+m đến khi được số dương thì dừng lại và lấy kq đó

- Nếu $x_i=0$ => không tồn tại phần tử nghịch đảo

	x	b	y
1	$x_1=m$	$b_1=0$	rỗng/*
2	$x_2=n$	$b_2=1$	$y_2=x_1 \text{ div } x_2$
$i\geq 3$	$x_i=x_{i-2} \bmod x_{i-1}$	$b_i=b_{i-2} - (b_{i-1}*y_{i-1})$	$y_i=x_{i-1} \text{ div } x_i$

Tính modulo nghịch đảo

- Tính $d \equiv e^{-1} \bmod \Phi(n)$
  $= 17^{-1} \bmod 3120$
- $d = (3120*k + 1)/17$

→ $d = 2753$ $(k=15)$

- $17^{-1} \bmod 3120$

$=-367+3120= 2753$

	x	b	y
1	3120	0	*
2	17	1	3120 div 17 =183
3	3120 mod 17 = 9	0-1*183=-183	17 div 9 =1
4	8	1-(-183)*1=184	1
5	1	-183-184*1=-367	

Tính modulo nghịch đảo

Tính 19^{-1} mod 26

19^{-1} mod 26 =11

	x	b	y
1	26	0	/
2	19	1	26 div 19=1
3	26 mod 19 =7	0-1*1=-1	2
4	5	3	1
5	2	-4	2
6	1	11	

Tính mod của lũy thừa lớn

- Tính **a^x mod n**
- Điều kiện dừng là $x_j=1 \rightarrow a^x \bmod n = d_j$

0	**x**	**a**	**$d_0=1$**
1	x	a	x_1 chẵn→ $d_1=d_0$ x_1 lẻ → $d_1=d_0*a_1 \bmod n$
$i\geq 2$	$x_i= x_{i-1}$ div 2	$a_i=(a_{i-1})^2 \bmod n$	x_i lẻ → $d_i=d_{i-1}*a_i \bmod n$ x_i chẵn→ $d_i=d_{i-1}$
j	$x_j=1$	tính a_j	tính d_j

Tính mod của lũy thừa lớn

- $c = m^e \bmod n = 65^{17} \bmod 3233 = 2790$

0	x	a	$d_0=1$
1	17	65	1*65 mod 3233=65
2	17 div 2 =**8**	65^2 mod 3233=992	65
3	8 div 2=4	992^2 mod 3233=1232	65
4	2	1547	65
5	1	789	65*789 mod 3233=**2790**

Tính mod của lũy thừa lớn

- Tính 15^{35} mod 79

0	x	a	d_0=1
1	35	15	15
2	17	67	57
3	8	65	57
4	4	38	57
5	2	22	57
6	1	10	57*10 mod 79=**17**

Tính mod của lũy thừa lớn

- Tính 35^{50} mod 67

0	x	a	d_0=1
1	**50**	35	1
2	25	19	19
3	12	26	19
4	6	6	19
5	3	36	14
6	1	23	54

3.4. Các hệ mã hóa khóa bất đối xứng

3.4.1. RSA

Ví dụ:Trong hệ mã hóa RSA cho: p = 37, q = 43, e = 59.

a. Hãy tìm khóa công khai Kp và khóa bí mật Ks của hệ mã trên?

b. Thực hiện mã hóa bản rõ m =60?

n=37*43=1591

Φ(n) =36*42=1512

e=59

3.4. Các hệ mã hóa khóa bất đối xứng

3.4.1. RSA

$d=e^{-1} \bmod \Phi(n) = 59^{-1} \bmod 1512$

$=-205+1512=1307$

Kp=(1591,59); Ks=(1591,1307)

	x	b	y
1	1512	0	/
2	59	1	25
3	37	-25	1
4	22	26	1
5	15	-51	1
6	7	77	2
7	1	-205	

3.4. Các hệ mã hóa khóa bất đối xứng

3.4.1. RSA

Mã hóa $c = m^e \bmod n$

$= 60^{59} \bmod 1591 = 66$

0	x	a	d=1
1	59	60	60
2	29	418	1215
3	**14**	**1305**	**1215**
4	7	655	325
5	3	1046	1067
6	1	1099	66

3.4. Các hệ mã hóa khóa bất đối xứng

3.4.1. ElGamal

- Hệ mật mã ElGamal được T. ElGamal đề xuất vào năm 1985
- Được xây dựng dựa trên độ phức tạp của bài toán tính logarit rời rạc
- Ứng dụng trong bảo mật, xác nhận và chữ ký điện tử

3.4. Các hệ mã hóa khóa bất đối xứng

3.4.1. ElGamal

- Thủ tục sinh khóa

- Chọn 1 số nguyên tố lớn p
- Chọn 1 số nguyên a thỏa mãn $0<a<p$ hay $a \epsilon Z_p^*$
- Chọn 1 số nguyên α, là phần tử nguyên thủy trong Z_p^*

  Tức là $0< \alpha<p$; UCLN(α,p)=1
- Tính số nguyên $\beta = \alpha^a \bmod p$
- Khóa $K_s = a$; $K_p = (p, \alpha, \beta)$

3.4. Các hệ mã hóa khóa bất đối xứng

3.4.1. ElGamal

- Thủ tục mã hóa ElGamal: Giả sử cần mã hóa thông điệp m
  - Chọn ngẫu nhiên 1 số nguyên k, k ϵ Z_{p-1} (0<=k<p-1)
  - Bản mã c=(y_1, y_2)
    - $y_1= \alpha^k \bmod p$;
    - $y_2= m^* \beta^k \bmod p= (m^*(\beta^k \bmod p)) \bmod p$
- Thủ tục giải mã ElGamal: Cho bản mã c= (y_1, y_2)
    - $m= y_2 * (y_1^{-a}) \bmod p$

3.4. Các hệ mã hóa khóa bất đối xứng

3.4.1. ElGamal

Ví dụ: Trong hệ mã hóa ELGAMAL

p = 179; α= 2; a = 101;

a. Tìm khóa công khai và khóa bí mật của hệ mã?

b. Chọn k ngẫu nhiên là 79, hãy mã hóa bản rõ m=67

3.4. Các hệ mã hóa khóa bất đối xứng

3.4.1. ElGamal

Tính số nguyên $\beta = \alpha^a \bmod p = 2^{101} \bmod 179$

Khóa Ks= a =101

Kp =(p, α, β) =(179, 2, 21)

	x	a	d=1
1	101	2	2
2	50	4	2
3	25	16	32
4	12	77	32
5	6	22	32
6	3	126	94
7	1	124	21

3.4. Các hệ mã hóa khóa bất đối xứng

3.4.1. ElGamal

- Bản mã $c=(y_1, y_2)$
- $y_1= \alpha^k \bmod p=2^{79} \bmod 179 =111$
- $y_2= m^* \beta^k \bmod p= 67*21^{79} \bmod 179$
  - Tính $21^{79} \bmod 179=54$
  - $y_2=67*54 \bmod 179=38$

Kết luận: c=(111, 38)

	x	a	d=1
1	79	2	2
2	39	4	8
3	19	16	128
4	9	77	11
5	4	22	11
6	2	126	11
7	1	124	111

	x	a	d=1
1	79	21	21
2	39	83	132
3	19	87	28
4	9	51	175
5	4	95	175
6	2	75	175
7	1	76	54

3.5. Chữ ký số, chứng chỉ số và PKI

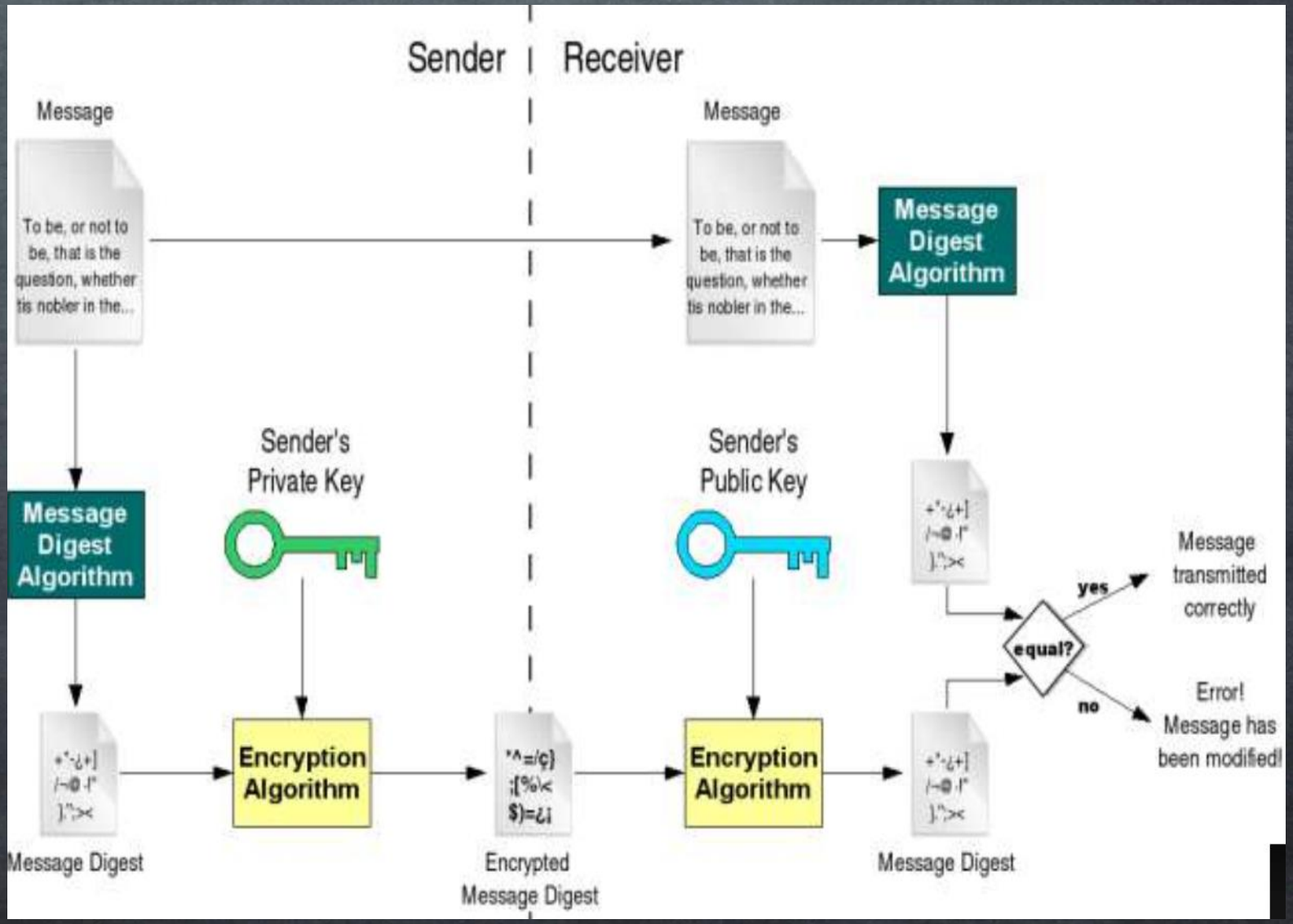
3.5.1. Chữ ký số

- Chữ ký số (Digital Signature) là một chuỗi dữ liệu liên kết với một thông điệp (message) và thực thể tạo ra thông điệp;
- Giải thuật tạo chữ ký số (Digital Signature generation algorithm) là một phương pháp sinh chữ ký số;
- Giải thuật kiểm tra chữ ký số (Digital Signature verification algorithm) là một phương pháp xác minh tính xác thực của chữ ký số, có nghĩa là nó thực sự được tạo ra bởi 1 bên chỉ định;
- Một hệ chữ ký số (Digital Signature Scheme) bao gồm giải thuật tạo chữ ký số và giải thuật kiểm tra chữ ký số.

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.1. Chữ ký số

- Sơ đồ ký và kiểm tra chữ ký số:



3.5. Chữ ký số, chứng chỉ số và PKI

3.5.1. Chữ ký số

- Các bước của quá trình ký:
  - Tính toán chuỗi đại diện thông điệp (MD)
  - Chuỗi đại diện được ký, sử dụng khóa bí mật của người gửi tạo chữ ký số (S)
  - Thông điệp ban đầu được ghép với chữ ký số thành thông điệp đã được ký (M+S)
  - Thông điệp đã được ký được gửi cho người nhận

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.1. Chữ ký số

- Các bước của quá trình kiểm tra chữ ký:
  - Tách riêng chữ ký số (S) và thông điệp ban đầu (M) từ thông điệp đã được ký (M+S)
  - Tính chuỗi đại diện thông điệp từ thông điệp ban đầu (M), thu được là MD1
  - Sử dụng khóa công khai của người gửi để giải mã chữ ký số (S), thu được MD2
  - So sáng MD1 và MD2:
    - Nếu MD1= MD2→ chữ ký hợp lệ, thông điệp toàn vẹn, thực sự xuất phát từ người gửi mong muốn
    - MD1 # MD2 → chữ ký không hợp lệ

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.2. Hệ chữ ký số RSA

- Thủ tục sinh khóa: Giống với mã hóa RSA

  Kp =(n, e), Ks=(n, d)

- Thủ tục ký: giả sử ký trên (chuỗi đại diện) thông điệp m

  - $sig_{Ks}(m)= m^d \bmod n=y$

- Thủ tục kiểm tra chữ ký:

  - $ver_{Kp}(m, y)$ = đúng ⇔ $m= y^e \bmod n$

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.2. Hệ chữ ký số RSA

VD1: Trong hệ chữ ký số RSA cho p = 31, q = 47, e = 67.

a) Xác định khóa công khai và khóa bí mật

b) Cho thông điệp m=100. Hãy tính chữ ký số trên m và kiểm tra chữ ký số đó.

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.2. Hệ chữ ký số RSA

VD1: Trong hệ chữ ký số RSA cho p = 31, q = 47, e = 67.

a) Xác định khóa công khai và khóa bí mật

n=31*47=1457

Ø(n) = (p-1)(q-1) =1380

e=67

d= e^{-1} mod Ø(n)= 67^{-1} mod 1380=103

	x	b	y
1	1380	0	/
2	67	1	20
3	40	-20	1
4	27	21	1
5	13	-41	2
6	1	103	

Kp=(1457, 67); Ks=(1457, 103)

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.2. Hệ chữ ký số RSA

VD1: Trong hệ chữ ký số RSA cho p = 31, q = 47, e = 67.

b) Cho thông điệp m=100. Hãy tính chữ ký số trên m và kiểm tra chữ ký số đó.

$sig_{Ks}(m) = m^d \bmod n$

$=100^{103} \bmod 1457 = 484$

	x	a	d=1
1	103	100	100
2	51	1258	498
3	25	262	803
4	12	165	803
5	6	999	803
6	3	1413	1093
7	1	479	484

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.2. Hệ chữ ký số RSA

VD1: Trong hệ chữ ký số RSA cho p = 31, q = 47, e = 67.

b) Cho thông điệp m=100. Hãy tính chữ ký số trên m và kiểm tra chữ ký số đó.

$ver_{Kp}(m, y)$ = đúng ⇔ $m = y^e \bmod n$

- Tính $m' = y^e \bmod n = 484^{67} \bmod 1457$
  - Có m'=m→ Chữ ký hợp lệ
  - Hoặc $ver_{Kp}(100, 484)$ = đúng

	x	a	d=1
1	67	484	484
2	33	1136	535
3	16	1051	535
4	8	195	535
5	4	143	535
6	2	51	535
7	1	1144	100

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.3. Hệ chữ ký số ElGamal

- Thủ tục sinh khóa: giống hệ mật mã ElGamal
  - $K_s = a$; $K_p = (p, \alpha, \beta)$
- Thủ tục ký: giả sử ký trên (chuỗi đại diện) thông điệp x
  - chọn k là số ngẫu nhiên $k \epsilon Z_{p-1}$ $(0<=k<p-1)$
  - $sig_{Ks}(x) = (y_1, y_2)$
    - $y_1 = \alpha^k \bmod p$
    - $y_2 = (x - a*y_1)*k^{-1} \bmod (p-1)$
- Thủ tục kiểm tra chữ ký:
  - $ver_{Kp}(x, (y_1, y_2))$= đúng $\Leftrightarrow \beta^{y1} * y_1^{y2} \equiv \alpha^x \pmod p$

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.3. Hệ chữ ký số ElGamal

VD: Trong hệ chữ ký số ELGAMAL cho p = 103; α = 2; a = 97; chọn k ngẫu nhiên là 79. Thông điệp x = 100.

Xác định chữ ký số trên x và kiểm tra chữ ký số đó.

- $sig_{Ks}(x) = (y_1, y_2)$
  - $y_1 = \alpha^k \bmod p = 2^{79} \bmod 103 = 49$

	x	a	d=1
1	79	2	2
2	39	4	8
3	19	16	25
4	9	50	14
5	4	28	14
6	2	63	14
7	1	55	49

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.3. Hệ chữ ký số ElGamal

- $sig_{Ks}(x) = (y_1, y_2)$
  - $y_1 = \alpha^k \bmod p = 2^{79} \bmod 103 = 49$
  - $y_2 = (x - a*y_1)*k^{-1} \bmod (p-1) = (100-97*49) * 79^{-1} \bmod 102$

    $z1 = (100-97*49) \bmod 102$

    $= -4653 \bmod 102 = -63+102 = 39$

    $z2 = 79^{-1} \bmod 102 = 31$

→ $y_2 = z1 * z2 \bmod (p-1) = 39*31 \bmod 102 = 87$

KL: $sig_{Ks}(100) = (49, 87)$

	x	b	y
1	102	0	/
2	79	1	1
3	23	-1	3
4	10	4	2
5	3	-9	3
6	1	31	

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.3. Hệ chữ ký số ElGamal

$ver_{Kp}(x, (y_1, y_2))$= đúng ⇔ $\beta^{y1} * y_1^{y2} \equiv \alpha^x \pmod p$

→$\beta^{y1} * y_1^{y2} \bmod p = \alpha^x \bmod p$

Tính $\beta = \alpha^a \bmod p = 2^{97} \bmod 103 = 29$

	x	a	d=1
1	97	2	2
2	48	4	2
3	24	16	2
4	12	50	2
5	6	28	2
6	3	63	23
7	1	55	29

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.3. Hệ chữ ký số ElGamal

VT = $\beta^{y1} * y_1^{y2} \bmod p = 97*30 \bmod 103 = 26$

$\beta^{y1} \bmod p = 29^{49} \bmod 103 = 97$

$y_1^{y2} \bmod p = 49^{87} \bmod 103 = 30$

	x	a	d=1
1	49	29	29
2	24	17	29
3	12	83	29
4	6	91	29
5	3	41	56
6	1	33	97

	x	a	d=1
1	87	49	49
2	43	32	23
3	21	97	68
4	10	36	68
5	5	60	63
6	2	98	63
7	1	25	30

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.3. Hệ chữ ký số ElGamal

VP= α^x mod p=2^{100} mod 103=26

Có VT=VP

Kết luận: Chữ ký nhận được là hợp lệ

Hoặc $ver_{Kp}(100, (49, 87))$= đúng

	x	a	d=1
1	100	2	1
2	50	4	1
3	25	16	16
4	12	50	16
5	6	28	16
6	3	63	81
7	1	55	26

3.5. Chữ ký số, chứng chỉ số và PKI

- Hệ mật mã khóa công khai: Bảo mật dữ liệu, không xác thực được người gửi
  - A gửi đi dữ liệu đã mã hóa cho B
  - A mã hóa bản rõ m sử dụng Kp của B
  - B giải mã bản mã c sử dụng Ks của B
- Hệ chữ ký số: Xác thực được người gửi, không bảo mật dữ liệu
  - A gửi đi thông điệp đã ký (M+S) cho B
  - A tạo chữ ký sử dụng khóa Ks của A
  - B ktra chữ ký sử dụng khóa Kp của A

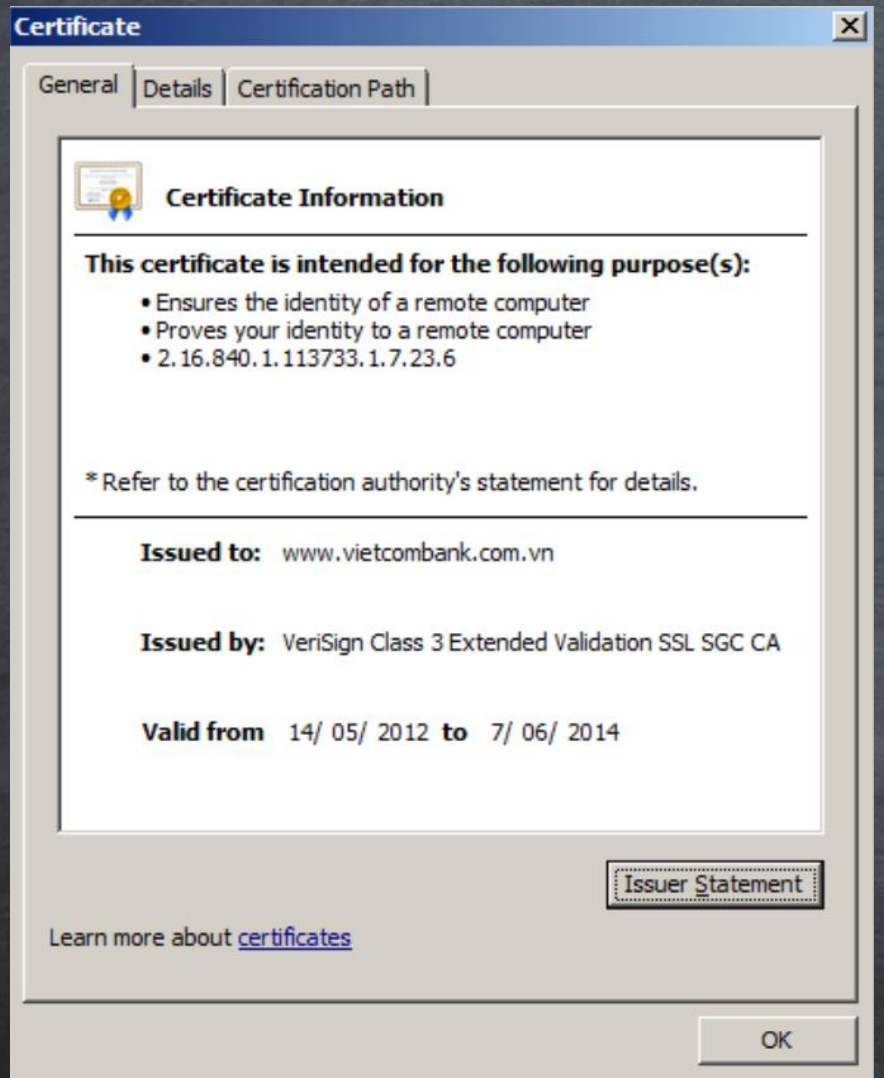
3.5. Chữ ký số, chứng chỉ số và PKI

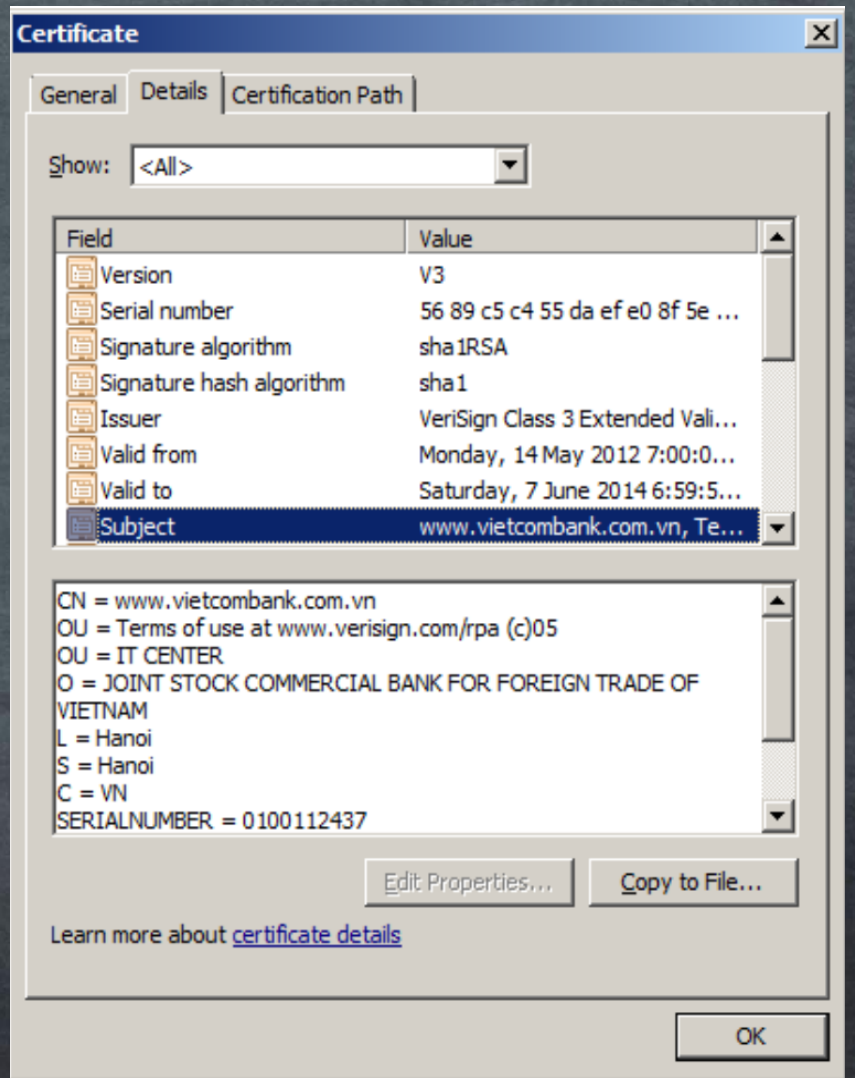
3.5.4. Chứng chỉ số và PKI

- Chứng chỉ số (Digital Certificate) còn gọi là chứng chỉ khóa công khai (Public key certificate), hay chứng chỉ nhận dạng (Identity certificate) là một tài liệu điện tử sử dụng một chữ ký số để liên kết một khóa công khai và thông tin nhận dạng của một thực thể:
  - Chữ ký số: là chữ ký của một bên thứ 3 tin cậy, thường gọi là CA – Certificate Authority;
  - Khóa công khai: là khóa công khai trong cặp khóa công khai của thực thể;
  - Thông tin nhận dạng: là tên, địa chỉ, tên miền hoặc các thông tin định danh của thực thể

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.4. Chứng chỉ số và PKI





3.5. Chữ ký số, chứng chỉ số và PKI

3.5.4. Chứng chỉ số và PKI

- Chứng chỉ số gồm các trường chính sau:
  - Serial Number: Số nhận dạng của chứng chỉ số;
  - Subject: Thông tin nhận dạng một cá nhận hoặc một tổ chức;
  - Signature Algorithm: Giải thuật tạo chữ ký;
  - Signature Hash Algorithm: Giải thuật tạo chuỗi băm cho tạo chữ ký;
  - Signature: Chữ ký của người/tổ chức cấp chứng chỉ;
  - Issuer: Người/tổ chức có thẩm quyền/tin cậy cấp chứng chỉ;

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.4. Chứng chỉ số và PKI

- Chứng chỉ số gồm các trường chính sau:
  - Issuer: Người/tổ chức có thẩm quyền/tin cậy cấp chứng chỉ;
  - Valid-From: Ngày bắt đầu có hiệu lực của chứng chỉ;
  - Valid-To: Ngày hết hạn sử dụng chứng chỉ;
  - Key-Usage: Mục đích sử dụng khóa (chữ ký số, mã hóa,…);
  - Public Key: Khóa công khai của chủ thể;
  - Thumbprint Algorithm: Giải thuật hash sử dụng để tạo chuỗi băm cho khóa công khai;
  - Thumbprint: Chuỗi băm tạo từ khóa công khai;

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.4. Chứng chỉ số và PKI

- Nội dung của trường Subject:
  - CN (Common Name): Tên chung, nhưng một tên miền được gán chứng chỉ;
  - OU (Organisation Unit): Tên bộ phận/phòng ban;
  - O (Organisation): Tổ chức/Cơ quan/công ty;
  - L (Location): Địa điểm/Quận huyện;
  - S (State/Province): Bang/Tỉnh/Thành phố;
  - C (Country): Đất nước.

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.4. Chứng chỉ số và PKI

- Đảm bảo an toàn cho giao dịch trên nền web:
  - Dùng chứng chỉ số cho phép website chạy trên SSL (tối thiểu máy chủ phải có chứng chỉ số): HTTP → HTTPS: toàn bộ thông tin chuyển giữa server và client được đảm bảo tính bí mật (sử dụng mã hóa khóa đối xứng), toàn vẹn và xác thực (sử dụng hàm băm có khóa MAC);
  - Chứng chỉ số để các bên xác thực thông tin nhận dạng của nhau.
- Chứng chỉ số có thể được sử dụng cho nhiều ứng dụng:
  - Email;
  - FTP;
  - Các ứng dụng khác.

3.5. Chữ ký số, chứng chỉ số và PKI

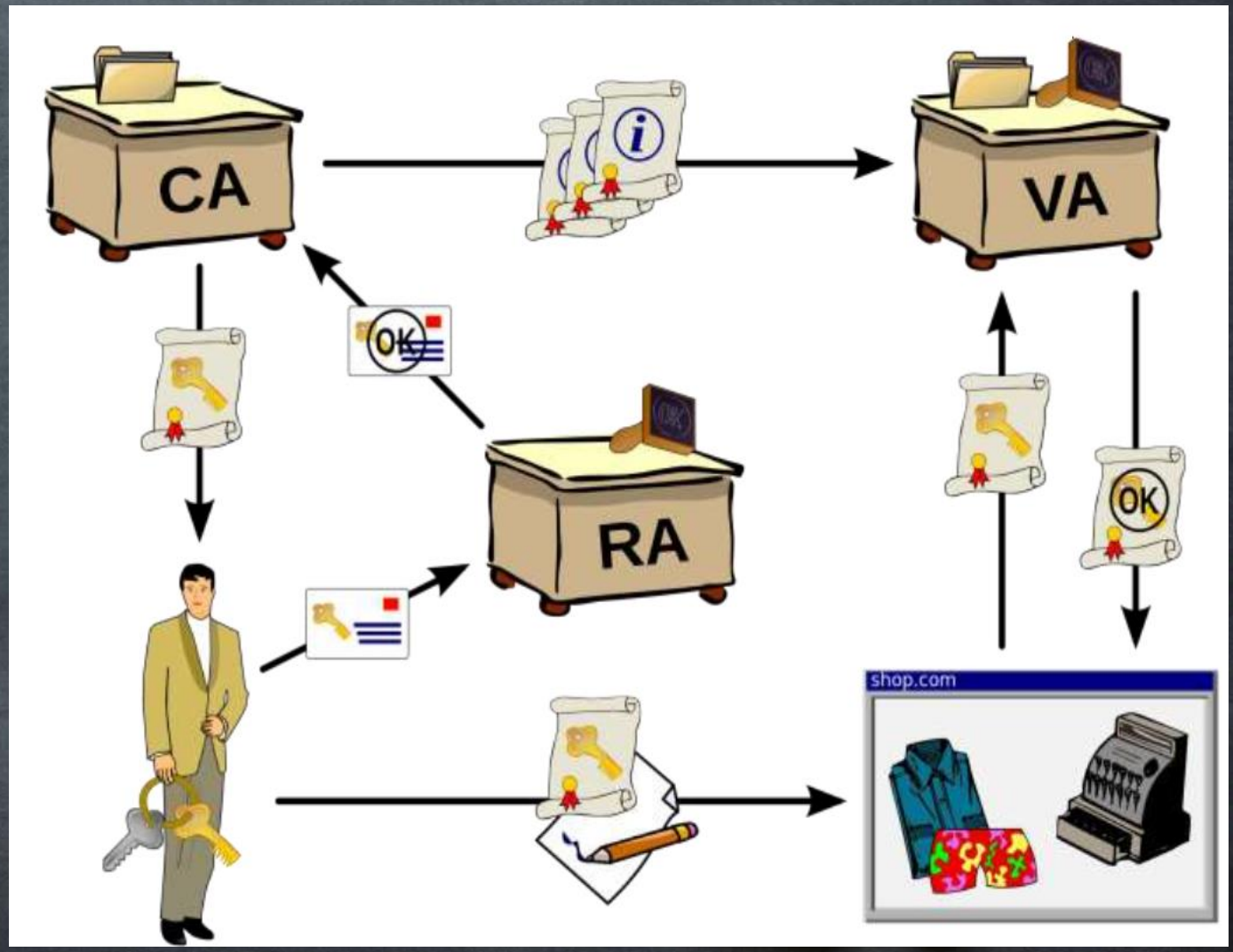
3.5.4. Chứng chỉ số và PKI

- Hạ tầng khóa công khai (Public-key infrastructure - PKI) là một tập các phần cứng, phần mềm, nhân lực, chính sách và các thủ tục để tạo, quản lý, phân phối, sử dụng, lưu trữ và thu hồi các chứng chỉ số;
- Một PKI gồm:
  - Certificate Authority (CA): Cơ quan cấp và kiểm tra chứng chỉ số;
  - Registration Authority (RA): Bộ phận kiểm tra thông tin nhận dạng của người dùng theo yêu cầu của CA;
  - Validation Authority (VA): Cơ quan xác nhận thông tin nhận dạng của người dùng thay mặt CA;
  - Central Directory (CD): Là nơi lưu danh mục và lập chỉ số các khóa;
  - Certificate Management System: Hệ thống quản lý chứng chỉ;
  - Certificate Policy: Chính sách về chứng chỉ;

3.5. Chữ ký số, chứng chỉ số và PKI

3.5.4. Chứng chỉ số và PKI

Sơ đồ cấp và sử dụng chứng chỉ số:



3.6. Quản lý khóa và phân phối khóa

1. Giới thiệu về quản lý và phân phối khóa
2. Các kỹ thuật phân phối khóa bí mật
3. Các kỹ thuật phân phối khóa công khai

3.6. Quản lý khóa và phân phối khóa

3.6.1. Giới thiệu về quản lý và phân phối khóa

- Quan hệ khóa (Keying relationship): là trạng thái mà trong đó các bên tham gia truyền thông chia sẻ dữ liệu chia sẻ (thường là khóa hoặc thành phần tạo ra khóa) để sử dụng cho các kỹ thuật mã hóa;
  - Các dữ liệu chia sẻ có thể là:
    - Khóa bí mật
    - Khóa công khai
    - Các giá trị khởi tạo
    - Các tham số bổ sung không bí mật.
- Quản lý khóa (Key management) là một tập các kỹ thuật cho phép thiết lập và duy trì các quan hệ khóa giữ các bên có thẩm quyền.

3.6. Quản lý khóa và phân phối khóa

3.6.1. Giới thiệu về quản lý và phân phối khóa

- Cụ thể, quản lý khóa gồm các kỹ thuật và thủ tục cho phép:
  - Khởi tạo các người dùng hệ thống (system users) trong một vùng (domain);
  - Sinh khóa, phân phối và cài đặt các dữ liệu khóa;
  - Kiểm soát việc sử dụng các dữ liệu khóa;
  - Cập nhật, thu hồi và hủy các dữ liệu khóa;
  - Lưu, sao lưu/khôi phục và lưu trữ các dữ liệu khóa.

3.6. Quản lý khóa và phân phối khóa

3.6.1. Giới thiệu về quản lý và phân phối khóa

- Quản lý khóa đóng vai trò quan trọng trong việc cung cấp các tính năng:
  - Tính bí mật
  - Toàn vẹn
  - Xác thực
  - Không thể chối bỏ
  - Chữ ký số.
- Quản lý khóa phù hợp sẽ đảm bảo cho các thông tin khóa được an toàn, đặc biệt khi có nhiều thực thể tham gia truyền thông.
  - Thông tin khóa an toàn → đảm bảo tính an toàn của hệ mã hóa.

3.6. Quản lý khóa và phân phối khóa

3.6.1. Giới thiệu về quản lý và phân phối khóa

- Các mối đe dọa đối với quản lý khóa:
  - Các khóa bí mật bị lộ;
  - Tính xác thực của các khóa bí mật và công khai bị thỏa hiệp (compromise). Tính xác thực bao gồm các hiểu biết và việc kiểm chứng thông tin nhận dạng của một bên mà khóa được chia sẻ;
  - Sử dụng trái phép các khóa bí mật và công khai:
    - Sử dụng các khóa đã hết hiệu lực;
    - Sử dụng các khóa sai mục đích.

3.6. Quản lý khóa và phân phối khóa

3.6.1. Giới thiệu về quản lý và phân phối khóa

- Chính sách an ninh và vấn đề quản lý khóa.
  - Quản lý khóa luôn được thực hiện trong khuôn khổ chính sách an ninh cụ thể;
- Chính sách an ninh mô tả các mục về quản lý khóa:
  - Các thực tế và thủ tục cần thực hiện trong các khía cạnh kỹ thuật và quản trị khóa tự động hoặc thủ công;
  - Trách nhiệm của các bên có liên quan;
  - Các bản ghi dữ liệu cần phải lưu để tạo các báo cáo về các vấn đề có liên quan đến an toàn khóa.

3.6. Quản lý khóa và phân phối khóa

3.6.1. Giới thiệu về quản lý và phân phối khóa

- Phân loại các lớp khóa theo khả năng sử dụng:
  - Khóa chủ (Master key):
    - Là các khóa ở mức cao nhất và không được bảo vệ bằng các kỹ thuật mật mã.
    - Các khóa chủ thường được chuyển giao trực tiếp và được bảo vệ bằng các cơ chế kiểm soát vật lý.
  - Khóa dùng cho trao đổi khóa (Key – encrypting keys):
    - Là những khóa được sử dụng để vận chuyển hoặc lưu trữ các khóa khác.
    - Các khóa này cũng có thể được bảo vệ bằng khóa khác.
  - Khóa dữ liệu (Data keys):
    - Là các khóa được sử dụng để mã hóa dữ liệu cho người dùng.
    - Thường là các khóa ngắn hạn.

3.6. Quản lý khóa và phân phối khóa

3.6.1. Giới thiệu về quản lý và phân phối khóa

- Phân loại các lớp khóa theo thời gian sử dụng:
  - Khóa dài hạn (long-term keys):
    - Là các khóa được sử dụng trong một khoảng thời gian dài;
    - Gồm: khóa chủ, khóa dùng cho trao đổi khóa, hoặc khóa dùng cho thỏa thuận khóa.
  - Khóa ngắn hạn:
    - Là các khóa được sử dụng trong một khoảng thời gian ngắn hoặc chỉ trong một phiên làm việc;
    - Gồm các khóa được trao đổi trong quá trình trao đổi khóa, thỏa thuận khóa, dùng để mã hóa dữ liệu của người dùng.

3.6. Quản lý khóa và phân phối khóa

3.6.2. Các kỹ thuật phân phối khóa bí mật

- Vấn đề phân phối n^2 khóa:
  - Nếu một hệ thống có n người dùng tham gia truyền thông sử dụng kỹ thuật mã hóa khóa đối xứng và mỗi cặp người dùng cần trao đổi thông tin an toàn:
    - Mỗi cặp người dùng cần chia sẻ một khóa bí mật duy nhất;
    - Mỗi người dùng cần sở hữu n-1 khóa bí mật;
    - Tổng số khóa cần quản lý trong hệ thống là $n(n-1)/2 \approx n^2$;
    - Số khóa cần quản lý sẽ rất lớn nếu số người dùng lớn.
  - Có thể sử dụng máy chủ trung tâm để quản lý và phân phối khóa.

3.6. Quản lý khóa và phân phối khóa

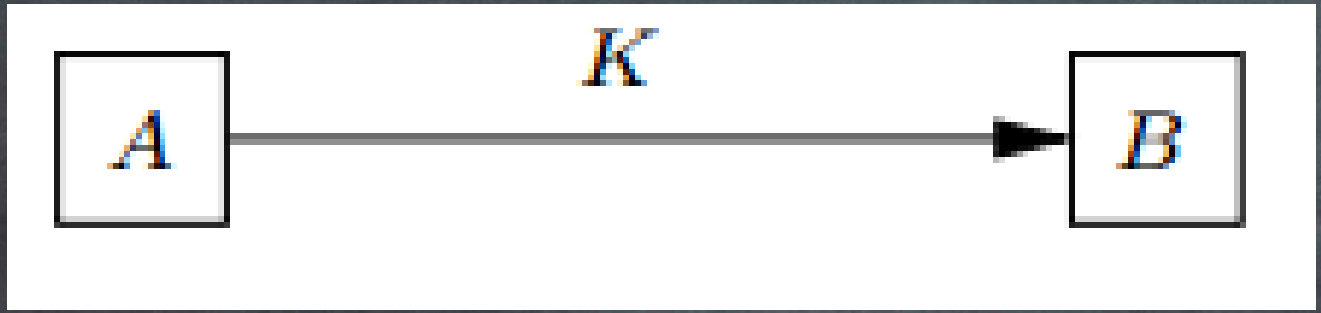
3.6.2. Các kỹ thuật phân phối khóa bí mật

- Các mô hình phân phối khóa đơn giản:
  - Phân phối khóa điểm – điểm (Point-to-point key distribution)
  - Trung tâm phân phối khóa (Key distribution center – KDC)
  - Trung tâm dịch hóa (Key translation center – KTC)

3.6. Quản lý khóa và phân phối khóa

3.6.2. Các kỹ thuật phân phối khóa bí mật

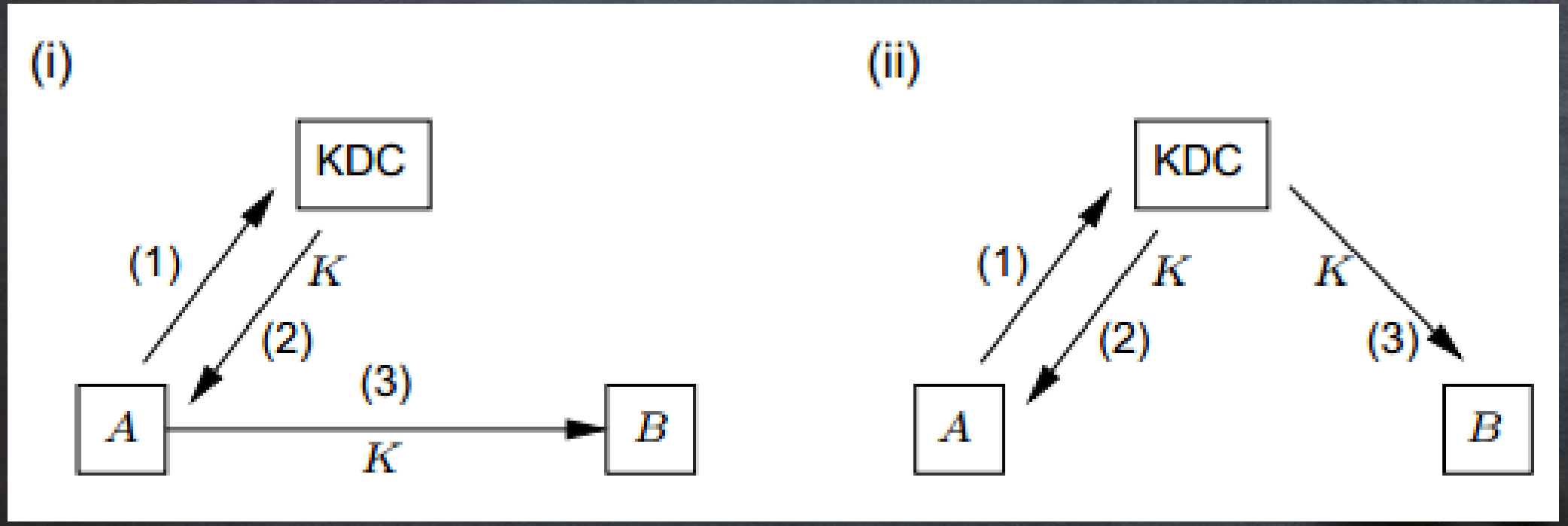
- Phân phối khóa điểm – điểm (Point-to-point key distribution):
  - Việc phân phối khóa chỉ liên quan trực tiếp đến 2 thực thể tham gia truyền thông.



3.6. Quản lý khóa và phân phối khóa

3.6.2. Các kỹ thuật phân phối khóa bí mật

- Trung tâm phân phối khóa (Key distribution center – KDC)



3.6. Quản lý khóa và phân phối khóa

3.6.2. Các kỹ thuật phân phối khóa bí mật

- Trung tâm phân phối khóa (Key distribution center – KDC)
  - KDC T được sử dụng để phân phối khóa;
  - Khởi tạo:
    - A sở hữu khóa dài hạn K_{AT} – chia sẻ với KDC;
    - B sở hữu khóa dài hạn K_{BT} – chia sẻ với KDC;
    - Trung tâm phân phối khóa T là một máy chủ tin cậy, cho phép hai bên A và B không trực tiếp chia sẻ thông tin khóa thiết lập kênh truyền thông an toàn sử dụng hai khóa dài hạn K_{AT} và K_{BT};
  - Gọi E là thủ tục mã hóa, D là thủ tục giải mã.

3.6. Quản lý khóa và phân phối khóa

3.6.2. Các kỹ thuật phân phối khóa bí mật

- Thủ tục phân phối khóa sử dụng KDC T:
  - A yêu cầu chia sẻ khóa với B;
  - Trung tâm phân phối khóa T sẽ tạo ra hoặc lấy khóa có sẵn K và mã hóa K thành $E_{K_{AT}}(K)$ và gửi cho A;
  - T cũng có thể gửi khóa cho B dưới dạng $E_{K_{BT}}(K)$ thông qua A (hình i);
  - T cũng có thể gửi khóa trực tiếp cho B dưới dạng $E_{K_{BT}}(K)$ (hình ii);
  - A nhận được $E_{K_{AT}}(K)$, giải mã sử dụng K_{AT} để có được K:

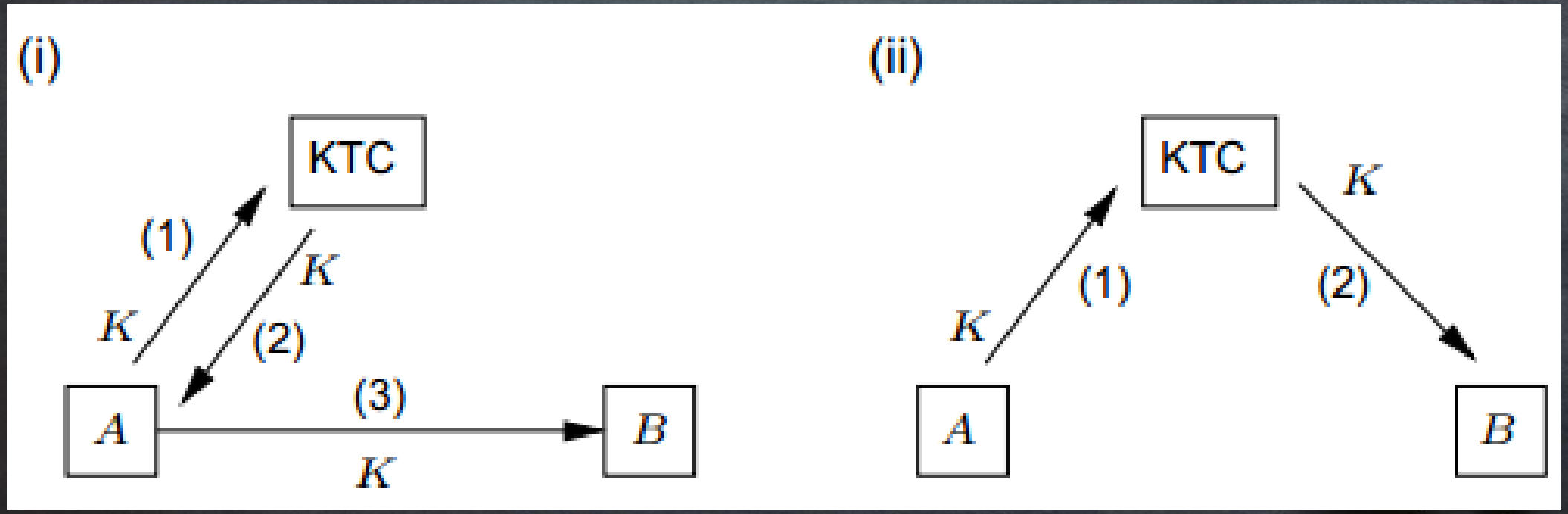
    $$D_{K_{AT}}(E_{K_{AT}}(K)) = K$$
  - B nhận được $E_{K_{BT}}(K)$, giải mã sử dụng K_{BT} để có được K:

    $$D_{K_{BT}}(E_{K_{BT}}(K)) = K$$

3.6. Quản lý khóa và phân phối khóa

3.6.2. Các kỹ thuật phân phối khóa bí mật

- Trung tâm dịch chuyển khóa (Key translation center – KTC)



3.6. Quản lý khóa và phân phối khóa

3.6.2. Các kỹ thuật phân phối khóa bí mật

- Trung tâm dịch chuyển khóa (Key translation center – KTC)
  - Vai trò của KTC tương tự KDC, tuy nhiên, một bên tham gia truyền thông sẽ cung cấp khóa phiên (session key).
  - Khởi tạo:
    - A sở hữu khóa dài hạn K_{AT} – chia sẻ với KTC T;
    - B sở hữu khóa dài hạn K_{BT} – chia sẻ với KTC T;
    - Trung tâm dịch khóa T là một máy chủ tin cậy, cho phép hai bên A và B không trực tiếp chia sẻ thông tin khóa thiết lập kênh truyền thông an toàn sử dụng hai khóa dài hạn K_{AT} và K_{BT}.
  - Gọi E là thủ tục mã hóa, D là thủ tục giải mã.

3.6. Quản lý khóa và phân phối khóa

3.6.2. Các kỹ thuật phân phối khóa bí mật

- Thủ tục phân phối khóa sử dụng KTC T:
  - A tạo ra khóa K và mã hóa K thành $E_{K_{AT}}(K)$ và gửi cho T;
  - T nhận được $E_{K_{AT}}(K)$, giải mã sử dụng K_{AT} thu được K:

    $$D_{K_{AT}}(E_{K_{AT}}(K)) = K$$
  - Sau đó T mã khóa K sử dụng K_{BT} để có $E_{K_{BT}}(K)$;
  - T có thể gửi khóa cho B dưới dạng $E_{K_{BT}}(K)$ thông qua A (hình i);
  - T cũng có thể gửi khóa trực tiếp cho B dưới dạng $E_{K_{BT}}(K)$ (hình ii);
  - B nhận được $E_{K_{BT}}(K)$, giải mã sử dụng K_{BT} để có được K:

    $$D_{K_{BT}}(E_{K_{BT}}(K)) = K$$

3.6. Quản lý khóa và phân phối khóa

3.6.2. Các kỹ thuật phân phối khóa bí mật

- So sánh KDC và KTC:
  - KDC cho phép sinh khóa tập trung;
  - KTC cho phép sinh khóa phân tán;
  - Cả KDC và KTC yêu cầu có một máy chủ tin cậy (trusted server).

3.6. Quản lý khóa và phân phối khóa

3.6.2. Các kỹ thuật phân phối khóa bí mật

- Ưu điểm của quản lý khóa tập trung (KDC+KTC)
  - Hiệu quả trong lưu trữ khóa: mỗi bên chỉ cần duy trì một khóa bí mật dài hạn với bên tin cậy (không phải với bên trao đổi thông tin);
  - Tổng số khóa dài hạn cần lưu trữ là n khóa (so với n^2 khóa).
- Nhược điểm của quản lý khóa tập trung (KDC+KTC)
  - Cả hệ thống có thể bị mất an toàn nếu trung tâm quản lý khóa bị thỏa hiệp (điều khiển);
  - Trung tâm quản lý khóa có thể thành điểm nút cổ chai;
  - Dịch vụ sẽ phải ngừng nếu trung tâm quản lý khóa gặp trục trặc;
  - Cần có một máy chủ tin cậy ở chế độ trực tuyến.

3.6. Quản lý khóa và phân phối khóa

3.6.3. Các kỹ thuật phân phối khóa công khai

- Các kỹ thuật phân phối khóa công khai thường giả thiết các bên tham gia truyền thông sơ hữu khóa công khai có tính xác thực (authentic public keys);
  - Là các khóa công khai được tạo và sử dụng hợp pháp.
- Việc phân phối khóa công khai cần đảm bảo tính xác thực của chủ thể khóa công khai:
  - Đảm bảo tính toàn vẹn;
  - Chủ thể luôn xác định.

3.6. Quản lý khóa và phân phối khóa

3.6.3. Các kỹ thuật phân phối khóa công khai

- Các kỹ thuật phân phối khóa công khai:
  - Trao đổi kiểu điểm-điểm thông qua kênh tin cậy;
  - Truy nhập trực tiếp vào danh mục công cộng (public-key registry);
  - Sử dụng một máy chủ trực tuyến tin cậy;
  - Sử dụng một máy chủ không trực tuyến và chứng chỉ;
  - Sử dụng các hệ thống đảm bảo tính xác thực với các tham số công cộng.

3.6. Quản lý khóa và phân phối khóa

3.6.3. Các kỹ thuật phân phối khóa công khai

- Trao đổi khóa công khai kiểu điểm-điểm thông qua kênh tin cậy:
  - Các bên trực tiếp trao đổi khóa công khai với nhau thông qua các kênh tin cậy như thư bảo đảm hoặc các phương tiện chuyển giao đảm bảo khác;
  - Có thể sử dụng với các trao đổi không thường xuyên;
  - Thích hợp với các hệ thống đóng kín hoặc cỡ nhỏ.
  - Nhược điểm:
    - Bất tiện do trễ lớn;
    - Các kênh tin cậy dùng riêng đắt tiền.

3.6. Quản lý khóa và phân phối khóa

3.6.3. Các kỹ thuật phân phối khóa công khai

- Trao đổi khóa công khai thông qua truy nhập trực tiếp vào danh mục công cộng:
  - Một CSDL công cộng tin cậy được thiết lập, bao gồm tên người dùng và khóa công khai tương ứng;
  - CSDL công cộng này có thể được vận hành bởi 1 bên tin cậy;
  - Người dùng có thể truy nhập khóa công khai từ CSDL này;
  - Một phương pháp thực hiện được sử dụng phổ biến là cây xác thực khóa công khai (Tree authentication of public keys).

3.6. Quản lý khóa và phân phối khóa

- Trao đổi khóa công khai thông qua sử dụng một máy chủ trực tuyến tin cậy:
  - Máy chủ trực tuyến tin cậy cung cấp truy nhập đến CSDL công cộng các khóa công khai;
  - Khóa công khai được ký sử dụng khóa riêng của máy chủ và gửi cho bên yêu cầu;
  - Kênh truyền không đòi hỏi phải bí mật;
  - Bên yêu cầu sử dụng khóa công khai của máy chủ để xác thực chữ ký của máy chủ và qua đó kiểm tra tính xác thực, toàn vẹn của khóa;
  - Nhược điểm:
    - Máy chủ phải luôn trực tuyến;
    - Máy chủ có thể trở thành điểm nút cổ chai.

3.6. Quản lý khóa và phân phối khóa

- Trao đổi khóa công khai thông qua sử dụng một máy chủ không trực tuyến và chứng chỉ:
  - Bên A liên hệ với một bên tin cậy (được gọi là Cơ quan chứng thực - Certification Authority (CA)) để đăng ký khóa công khai của mình và nhận được chữ ký xác nhận khóa công khai của CA;
  - CA cấp một chứng chỉ (Certificate) cho khóa công khai của A: chứng chỉ kết hợp khóa công khai của A với thông tin định danh của A;
  - Khi A đã có chứng chỉ khóa công khai (Public key certificate), A có thể gửi khóa công khai cho các bên có liên quan bằng cách gửi chứng chỉ khóa công khai.
  - Chứng chỉ khóa công khai cũng có thể được đưa vào danh mục công cộng và người dùng có thể truy nhập.