

- Ưu điểm:
  - Linh hoạt, phù hợp nhu cầu giao tiếp đa dạng
  - Cho phép những nhóm người sử dụng khác nhau có thể tự do phát triển và thực thi các chính sách và chuẩn khác nhau
  - Tính cạnh tranh cao
  - Khắc phục được nhược điểm của mô hình phân cấp
- Nhược điểm:
  - Số xác thực chéo lớn ( $n^2$ )
  - Phức tạp và khó quản lý

## Chương 4

# CÁC HỆ MẬT MÃ

- Vai trò của mật mã trong An toàn thông tin
- Mật mã đối xứng
- Hệ mật bất đối xứng
- Hàm băm một chiều (One Way Hash function)
- Chữ ký số (Digital signature).

## 4.1 Vai trò của mật mã trong An toàn thông tin

- Mật mã học (Cryptography)
  - Là một ngành khoa học chuyên nghiên cứu các phương pháp để giữ thông tin được an toàn.
  - Là việc sử dụng các kỹ thuật thích hợp để biến đổi một bản thông điệp có ý nghĩa thành một dãy mã ngẫu nhiên để liên lạc với nhau giữa người gửi và người nhận.
- Mã hóa và giải mã gồm:
  - Bản rõ (plaintext or cleartext): Chứa các chuỗi ký tự gốc, thông tin trong bản rõ là thông tin cần mã hoá để giữ bí mật.
  - Bản mã (ciphertext): Chứa các ký tự sau khi đã được mã hoá, mà nội dung của nó được giữ bí mật.

## Vai trò của mật mã trong An toàn thông tin

- Mã hoá (Encryption): quá trình che dấu thông tin bằng phương pháp nào đó để làm ẩn nội dung bên trong trước khi gửi.
- Giải mã (Decryption): quá trình biến đổi ngược lại từ bản mã nhận được trở thành bản rõ ban đầu.



99

## Vai trò của mật mã trong An toàn thông tin

- Vai trò của hệ mật mã
  - Che dấu được nội dung của thông tin, chống truy nhập không đúng quyền hạn.
  - Tạo các yếu tố xác thực thông tin, đảm bảo thông tin lưu hành trong hệ thống đến người nhận hợp pháp là xác thực (Authenticity)
  - Đảm bảo không có hiện tượng mạo danh để thực hiện truyền nhận thông tin trên mạng.

100

## Vai trò của mật mã trong An toàn thông tin



101

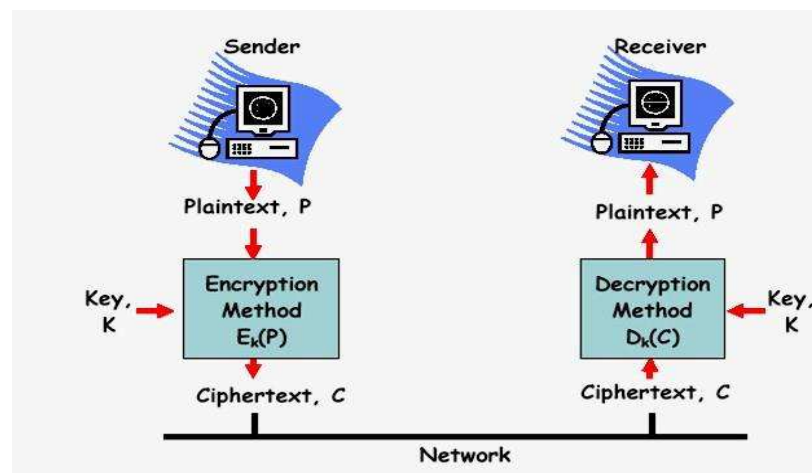
## 4.2 Mật mã đối xứng

- Còn gọi là hệ mật mã khóa bí mật: những hệ mật mã dùng chung một khoá cả trong quá trình mã hoá dữ liệu và giải mã dữ liệu → vì vậy yêu cầu cần thiết khoá phải được giữ bí mật tuyệt đối
- Người gửi và người nhận chia sẻ cùng một khoá dùng chung "K" được trao đổi bí mật với nhau
- Đối xứng: khóa để mã hóa và khóa để giải mã là một

102

- Các khái niệm trong mật mã đối xứng:
  - **Bản rõ** (M) được gọi là bản tin gốc, có thể được chia nhỏ và có kích thước phù hợp
  - **Khoá** (K) là thông tin tham số dùng để mã hoá, độc lập với bản rõ và có độ dài phù hợp với yêu cầu bảo mật
  - **Mã hóa**: thuật toán (E) chuyển bản rõ thành bản mã, dựa trên khoá K.
  - **Bản mã** (C) là bản tin gốc đã được mã hoá
  - **Giải mã**: thuật toán (D) chuyển bản mã thành bản rõ, dựa vào khoá (K), là quá trình ngược lại của mã hóa
- Định nghĩa: một hệ mã đối xứng (K,M,C) là hệ mã bao gồm hai thuật toán (E,D) sao cho:
  - $E: K \times M \rightarrow C$
  - $D: K \times C \rightarrow M$
  - $\forall m \in M, k \in K: D(k, E(k,m)) = m$

103



104

- Các kiểu mã hóa đối xứng
  - Phép thế: thay thế các ký tự trên bản rõ bằng các ký tự khác
  - Hoán vị: thay đổi vị trí các ký tự trong bản rõ, tức là thực hiện hoán vị các ký tự của bản rõ.
  - Kết hợp cả hai kiểu thay thế và hoán vị các ký tự của bản rõ
- Cách xử lý bản rõ
  - Theo khối: dữ liệu được chia thành từng khối có kích thước xác định và áp dụng thuật toán mã hóa với tham số khóa cho từng khối.
  - Theo dòng: từng phần tử đầu vào được xử lý liên tục tạo phần tử đầu ra tương ứng.

105

- Một số hệ mật đối xứng cổ điển
  - **Mã thay thế** là phương pháp mà từng kí tự (nhóm kí tự) trong bản rõ được thay thế bằng một kí tự (một nhóm kí tự) khác để tạo ra bản mã. Bên nhận chỉ cần thay thế ngược lại trên bản mã để có được bản rõ ban đầu
    - Mã Caesar
    - Mã thay thế đơn bảng (Monoalphabetic Substitution)
    - Mã Playfair
    - Mã Hill
    - Mã Vigenere

106

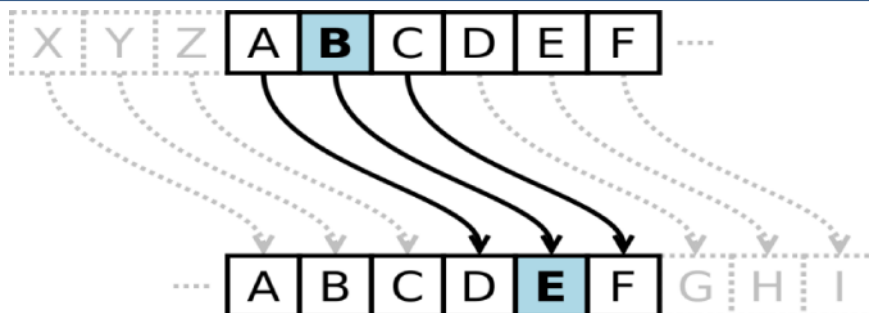
- Một số hệ mật đối xứng cổ điển
  - **Mã hoán vị:** các kí tự trong bản rõ vẫn được giữ nguyên, nhưng được hoán vị vị trí để tạo thành bản mã.
    - Mã Rail Fence
    - Mã dịch chuyển dòng

- Do Julius Caesar đề xuất, lần đầu tiên được sử dụng trong quân sự
- Thuật toán mô tả: thay mỗi chữ trong bản rõ bằng chữ đứng sau nó k vị trí trong bảng chữ cái
- Ví dụ với khóa  $k = 3$ :
  - Bản rõ “HELP ME” được mã hóa thành “KHOSPH”.

Chữ ban đầu: 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

Chữ thay thế: 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

## Mã Caesar



- Ví dụ 2: Nếu với khóa  $k = 3$ 
  - “TRY AGAIN” được mã hóa thành “WUB DJDLQ”

Chữ ban đầu: 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

Chữ thay thế: 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

109

## Mã Caesar (tt)

- Nếu gán số thứ tự cho mỗi chữ trong bảng chữ cái.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Phương pháp Caesar được biểu diễn như sau: với mỗi chữ cái  $p$  thay bằng chữ mã hóa  $C$ , trong đó:  

$$C = (p + k) \bmod 26$$
 (trong đó  $\bmod$  là phép chia lấy số dư)
- Và quá trình giải mã đơn giản là:  

$$p = (C - k) \bmod 26$$
  - $k$  được gọi là khóa

110



## Mã Caesar (tt)

- Nhận xét: không an toàn vì k chỉ nhận 25 giá trị.
  - Ví dụ từ bảng mã:  
PHHW PH DIWHU WKH WRJD SDUWB
  - Có thể thử với các giá trị của k = 1 cho đến k=25:

KEY	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1	oggv	og	chvgt	vjg	vqic	rctva
2	nffu	nf	bgufs	uif	uphb	qbsuz
3	<b>meet</b>	<b>me</b>	<b>after</b>	<b>the</b>	<b>toga</b>	<b>party</b>
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrpc	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	ojbv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr

111

## Mã Caesar – Bài tập

- Cho k = 7, N = 26, mã hóa văn bản P = GOOD TIME
- Cho k = 9, n = 26, mã hóa văn bản P = MY BABY
- Cho k = 15, n = 26, mã hóa văn bản P = HELLO MY FRIEND
- Cho k = 6, n = 26, giải mã văn bản C = JGONUISU
- Cho k = 18, n = 26, giải mã với C = UGFYFYZWZLZGFYLA

112

## Mã hóa thay thế đơn bảng

- Khắc phục yếu điểm của phương pháp Caesar:

- Không dịch chuyển  $k$  vị trí của các chữ cái mà mỗi chữ của bản rõ được ánh xạ đến một chữ khác nhau của bản mã. Ví dụ:

Chữ ban đầu: 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

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

Như vậy bản rõ meet me after the toga party

được mã hóa thành: NJJU NJ ZRUJM UKJ UVSZ DZMUE

- **Nhận xét:**

- Không gian khóa =  $26!$  → khá lớn → tấn công phá mã vét cạn khóa là bất khả thi (có an toàn với các máy tính hiện đại ?)
- Không thật sự an toàn vì tần suất xuất hiện của các chữ trong bản rõ và các chữ tương ứng trong bản mã là như nhau → có thể đoán được ('E': 12.7%, 'T': 9.1%, 'A': 8.1%,...)

113

## Các hệ mật mã cổ điển Hệ mã hóa thay thế

### Phân tích tần số

Ký tự:  $E > T > R > N > I > O > A > S$

Nhóm 2 ký tự (digraph):  $TH > HE > IN > ER > RE > ON > AN > EN$

Nhóm 3 ký tự (Trigraph):  $THE > AND > TIO > ATI > FOR > THA > TER > RES$

114

## Thống kê tham khảo

Chữ cái (%)		Cụm 2 chữ (%)		Cụm 3 chữ (%)		Từ (%)	
E	13.05	TH	3.16	THE	4.72	THE	6.42
T	9.02	IN	1.54	ING	1.42	OF	4.02
O	8.21	ER	1.33	AND	1.13	AND	3.15
A	7.81	RE	1.30	ION	1.00	TO	2.36
N	7.28	AN	1.08	ENT	0.98	A	2.09
I	6.77	HE	1.08	FOR	0.76	IN	1.77
R	6.64	AR	1.02	TIO	0.75	THAT	1.25
S	6.46	EN	1.02	ERE	0.69	IS	1.03
H	5.85	TI	1.02	HER	0.68	I	0.94
D	4.11	TE	0.98	ATE	0.66	IT	0.93
L	3.60	AT	0.88	VER	0.63	FOR	0.77
C	2.93	ON	0.84	TER	0.62	AS	0.76
F	2.88	HA	0.84	THA	0.62	WITH	0.76
U	2.77	OU	0.72	ATI	0.59	WAS	0.72
M	2.62	IT	0.71	HAT	0.55	HIS	0.71
P	2.15	ES	0.69	ERS	0.54	HE	0.71
Y	1.51	ST	0.68	HIS	0.52	BE	0.63
W	1.49	OR	0.68	RES	0.50	NOT	0.61
G	1.39	NT	0.67	ILL	0.47	BY	0.57
B	1.28	HI	0.66	ARE	0.46	BUT	0.56
V	1.00	EA	0.64	CON	0.45	HAVE	0.55
K	0.42	VE	0.64	NCE	0.45	YOU	0.55
X	0.30	CO	0.59	ALL	0.44	WHICH	0.53
J	0.23	DE	0.55	EVE	0.44	ARE	0.50
Q	0.14	RA	0.55	ITH	0.44	ON	0.47
Z	0.09	RO	0.55	TED	0.44	OR	0.45

115

## Mã Vigenere

- Phương án mã hóa thay thế đa bảng
- Thực chất là việc tiến hành đồng thời dùng nhiều mã Caesar cùng một lúc trên bản rõ với nhiều khoá khác nhau.
- Để mã hóa một bản tin thì cần có một khóa có chiều dài bằng chiều dài bản tin.
- Khóa thường là một cụm từ được viết lặp lại cho đến khi có chiều dài bằng chiều dài bản tin. Ví dụ:
  - Bảng rõ (plain text): DOTNETSPIDER
  - Khóa: PAUL: PAULPAULPAUL

116

• Ví dụ 1:

- plain text:  
“DOTNETSPIDER  
IS A LEADING  
WEBSITE FOR  
DOT NET  
COMMUNITY”
- Key: “PAUL”
- Cipher text:  
“SONYTTMAXDYC  
XS U WTAXTCG  
QPQSCET FIC  
SON YTT  
WZBMOYXTS”.

TEXT REFERENCE	
	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

- plain text:  
“DOTNETSPIDE  
R IS A LEADING  
WEBSITE FOR  
DOT NET  
COMMUNITY”
- Key: “PAUL”
- Cipher text:  
“SONYTTMAXDY  
C XS U  
WTAXTCG  
QPQSCET FIC  
SON YTT  
WZBMOYXTS”.

TEXT REFERENCE	
	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

## Mã Vigenere (tt)

### • Ví dụ 2:

plaintext: wearediscoveredsaveyourself  
key: DECEPTIVEDECEPTIVEDECEPTIVE  
ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

key	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

119

## Mã Vigenere (tt)

### • Nhận xét:

- Có sự lặp lại các từ trong khóa, ví dụ từ *DECEPTIVE* được lặp đi lặp lại nhiều lần.
- Tồn tại một mối liên quan giữa bản rõ và bản mã, ví dụ cụm từ **red** trong bản rõ được lặp lại thì cụm từ **VTW** cũng được lặp lại trong bản mã.

plaintext: wearediscoveredsaveyourself  
key: DECEPTIVEDECEPTIVEDECEPTIVE  
ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

### → Khắc phục:

- Sử dụng khóa ngẫu nhiên, là khóa có chiều dài bằng chiều dài của bản rõ, mỗi khóa chỉ sử dụng một lần.
- Sử dụng hai khóa

120

## Mã Vigenere (tt)

- Cho  $k = \text{KEY}$ ,  $N = 26$ , mã hóa văn bản

**P = TRUONG DAI HOC MO**

- Cho  $k = \text{KEY}$ ,  $N = 26$ , giải mã văn bản:

**P = ULM KGM XKL QLC DLM XKR SR**

- Cho  $k = \text{KEY}$ ,  $N = 22$ , mã hóa văn bản

**P = KHOACONGNGHETHONGTIN**

121

## Mã Vigenere (tt)

- Cho  $k = \text{KEY}$ ,  $N = 26$ , giải mã văn bản

**P = ULM KGM XKL QLC DLM XKR SR**

Key	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Chữ ban đầu:	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

- Giải mã:  $D_k(P) = P_1 - k_1, P_2 - k_2, \dots, P_M - k_M \bmod N$

C	20	11	12	10	6	12	23	10	11	16	11	2	3	11	12	23	10	17	18	17
K	10	4	24	10	4	24	10	4	24	10	4	24	10	4	24	10	4	24	10	4
P	10	7	14	0	2	14	13	6	13	6	7	4	19	7	14	13	6	19	8	13

122

## Mã Vigenere (tt)

- ❑ Cho  $k = \text{TRUONG}$ ,  $N = 26$ , giải mã văn bản, dùng thuật mã Vigenere với  $C = \text{MIOCAMWRCVBIFF}$
- ❑ Cho  $k = \text{KHOA}$ ,  $N = 26$ , giải mã văn bản, dùng thuật mã Vigenere với  $C = \text{WRIHNUMIOQGARVH}$
- ❑ Cho  $k = \text{SECRET}$ ,  $N = 26$ , mã hóa văn bản, dùng thuật mã Vigenere  $P = \text{KHOACONGNGHETHONGTIN}$
- ❑ Cho  $k = \text{MORNACHY}$ ,  $N = 26$ , mã hóa văn bản, dùng thuật mã Vigenere  $P = \text{ANTOANBAOMATTHONGTIN}$

123

## Mã Vigenere (tt)

Key	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Chữ ban đầu:	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

### • Sử dụng khóa ngẫu nhiên:

– Ví dụ: bản tin P được mã hóa với khóa K1

Bản tin P: **wearediscoveredsaveyourself**  
 Khóa K1: **FHWYKLVKVKXCVKDJSFSAPXZCVP**  
 Bản mã C: **BLWPOODEMJFBTZNJVJNJQOJORGGU**

– Sau đó bản mã C được giải mã với khóa K2, K3

Bản mã C: **BLWPOODEMJFBTZNJVJNJQOJORGGU**  
 Khóa K2: **IESRLKBWJFCIFZUCJLZXAXAAPSY**  
 Bản giải mã: **theydecidedtoattacktomorrow**  
*(they decided to attack tomorrow)*

Bản mã C: **BLWPOODEMJFBTZNJVJNJQOJORGGU**  
 Khóa K3: **FHAHDDRAIQFIASJGJWQSVVBIAZB**  
 Bản giải mã: **wewillmeetatthepartytonight**  
*(we will meet at the party tonight)*

124

- Sử dụng hai khóa:
  - Ví dụ: bổ sung khóa Key2: "SPIDER"

		TEXT REFERENCE						
		SPID	ERAB	CFGH	JKLM	NOQT	UVWX	YZ
P A S S W O R D	S	SPID	ERAB	CFGH	JKLM	NOQT	UVWX	YZ
	P	PIDE	RABC	FGHJ	KLMN	OQTU	VWXY	ZS
	I	IDER	ABCF	GHJK	LMNO	QTUV	WXYZ	SP
	D	DERA	BCFG	HJKL	MNOQ	TUVW	XYZS	PI
	E	ERAB	CFGH	JKLM	NOQT	UVWX	YZSP	ID
	R	RABC	FGHJ	KLMN	OQTU	VWXY	ZSPI	DE
	A	ABCF	GHJK	LMNO	QTUV	WXYZ	SPID	ER
	B	BCFG	HJKL	MNOQ	TUVW	XYZS	PIDE	RA
	C	CFGH	JKLM	NOQT	UVWX	YZSP	IDER	AB
	F	FGHJ	KLMN	OQTU	VWXY	ZSPI	DERA	BC
R E F E R E N C E	G	GHJK	LMNO	QTUV	WXYZ	SPID	ERAB	CF
	H	HJKL	MNOQ	TUVW	XYZS	PIDE	RABC	FG
	J	JKLM	NOQT	UVWX	YZSP	IDER	ABCF	GH
	K	KLMN	OQTU	VWXY	ZSPI	DERA	BCFG	HJ
	L	LMNO	QTUV	WXYZ	SPID	ERAB	CFGH	JK
	M	MNOQ	TUVW	XYZS	PIDE	RABC	FGHJ	KL
	N	NOQT	UVWX	YZSP	IDER	ABCF	GHJK	LM
	O	OQTU	VWXY	ZSPI	DERA	BCFG	HJKL	MN
	Q	QTUV	WXYZ	SPID	ERAB	CFGH	JKLM	NO
	T	TUVW	XYZS	PIDE	RABC	FGHJ	KLMN	OQ
	U	UVWX	YZSP	IDER	ABCF	GHJK	LMNO	QT
	V	VWXY	ZSPI	DERA	BCFG	HJKL	MNOQ	TU
	W	WXYZ	SPID	ERAB	CFGH	JKLM	NOQT	UV
	X	XYZS	PIDE	RABC	FGHJ	KLMN	OQTU	VW
	Y	YZSP	IDER	ABCF	GHJK	LMNO	QTUV	WX
	Z	ZSPI	DERA	BCFG	HJKL	MNOQ	TUVW	XY

125

## Mã Vigenere (tt)

- Sử dụng hai khóa
  - Ví dụ:
    - plain text: "WEBSITE"
    - Key: "PAUL"
    - Key2: "SPIDER"

		TEXT REFERENCE						
		SPID	ERAB	CFGH	JKLM	NOQT	UVWX	YZ
P A S S W O R D	P	PIDE	RABC	FGHJ	KLMN	OQTU	VWXY	ZS
	A	ABCF	GHJK	LMNO	QTUV	WXYZ	SPID	ER
	L	LMNO	QTUV	WXYZ	SPID	ERAB	CFGH	JK
	U	UVWX	YZSP	IDER	ABCF	GHJK	LMNO	QT

126



## Mã Vigenere (tt)

- Sử dụng hai khóa
- Ví dụ:
  - plain text: “WEBSITE”
  - Key: “PAUL”
  - Key2: “SPIDER”

		TEXT REFERENCE							
		SPID	ERAB	CFGH	JKLM	NOQT	UVWX	YZ	
P A S S W O R D	P	PIDE	RABC	FGHJ	KLMN	OQTU	VWXY	ZS	
	A	ABCF	GHJK	LMNO	QTUV	WXYZ	SPID	ER	
	L	LMNO	QTUV	WXYZ	SPID	ERAB	CFGH	JK	
	U	UVWX	YZSP	IDER	ABCF	GHJK	LMNO	QT	

127

## Mã Vigenere (tt)

- Sử dụng hai khóa. Ví dụ: plain text: “WEBSITE”
  - Key: “PAUL”
  - Key2: “SPIDER”
  - → cipher text: “XGPLDZY”

		TEXT REFERENCE							
		SPID	ERAB	CFGH	JKLM	NOQT	UVWX	YZ	
P A S S W O R D	P	PIDE	RABC	FGHJ	KLMN	OQTU	VWXY	ZS	
	A	ABCF	GHJK	LMNO	QTUV	WXYZ	SPID	ER	
	L	LMNO	QTUV	WXYZ	SPID	ERAB	CFGH	JK	
	U	UVWX	YZSP	IDER	ABCF	GHJK	LMNO	QT	

		TEXT REFERENCE							
		SPID	ERAB	CFGH	JKLM	NOQT	UVWX	YZ	
P A S S W O R D	P	PIDE	RABC	FGHJ	KLMN	OQTU	VWXY	ZS	
	A	ABCF	GHJK	LMNO	QTUV	WXYZ	SPID	ER	
	L	LMNO	QTUV	WXYZ	SPID	ERAB	CFGH	JK	
	U	UVWX	YZSP	IDER	ABCF	GHJK	LMNO	QT	

128

## Mã Playfair

- Mã thay thế đa ký tự: Xem hai ký tự đứng sát nhau là một đơn vị mã hóa, hai ký tự này được thay thế cùng lúc bằng hai ký tự khác
- Ma trận khóa Playfair: chọn một từ làm khóa, với điều kiện trong từ khóa đó không có chữ cái nào bị lặp → lập ma trận Playfair (5 x 5) dựa trên từ khóa đã cho và gồm các chữ trên bảng chữ cái, được sắp xếp theo thứ tự như sau:
  - Viết các chữ của từ khóa vào các hàng của ma trận bắt từ hàng thứ nhất.
  - Nếu ma trận còn trống, viết các chữ khác trên bảng chữ cái chưa được sử dụng vào các ô còn lại. Có thể viết theo một trình tự qui ước trước, chẳng hạn từ đầu bảng chữ cái cho đến cuối.
  - Tiếng Anh có 26 chữ cái → thiếu một ô. Thông thường ta dồn hai chữ nào đó vào một ô chung, chẳng hạn I và J

129

## Mã Playfair (tt)

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

- Ví dụ: sử dụng **MONARCHY** làm từ khóa
- Bản rõ được tách ra thành các cặp ký tự.
  - Nếu hai ký tự trong một cặp giống nhau thì thêm ký tự X vào giữa  
Ví dụ: từ **balloon** được tách thành **ba lx lo on**
  - Nếu thừa một ký tự lẻ thì thêm ký tự **X** vào cuối
- Việc mã hóa từng cặp được thực hiện theo quy tắc:
  - Nếu hai ký tự trong cặp thuộc cùng một hàng, thì mỗi ký tự được thay bằng chữ ở phía bên phải nó trong cùng hàng của ma trận khóa (cuộn vòng quanh từ cuối về đầu), Ví dụ: **ar** → **RM**.
  - Nếu hai ký tự cặp thuộc cùng một cột, thì mỗi ký tự được thay bằng chữ ở phía bên dưới nó trong cùng cột của ma trận khóa (cuộn vòng quanh từ cuối về đầu). Ví dụ: **mu** → **CM**.
  - Nếu hai ký tự tạo thành một hình chữ nhật → được thay bằng 2 ký tự cùng dòng ở hai đỉnh còn lại.  
Ví dụ: **hs** → **BP** (B cùng dòng với H và P cùng dòng với S);  
**ea** → **IM** (hoặc JM)

130

- Ví dụ:
  - Với khóa là: PASSWORD  
Hãy mã hóa chuỗi văn bản THIS IS SECURITY TEXT
  - Với khóa là: PASSWORD  
Hãy mã hóa chuỗi văn bản AN TOAN HE THONG
  - Với khóa là: PASSWORD  
Mã hóa chuỗi văn bản AN TOAN THONG TIN

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

- Cho  $k = \text{MONARCHY}$ , mã hóa văn bản  $P = \text{ABC}$
- Cho  $k = \text{MONARCHY}$ , mã hóa văn bản  $P = \text{ADC}$
- Cho  $k = \text{MONARCHY}$ , mã hóa văn bản  $P = \text{TRUONGDAIHOCMO}$
- Cho  $k = \text{MONARCHY}$ , mã hóa văn bản  $P = \text{ANTOANTHONGTIN}$
- Cho  $k = \text{KEY}$ , giải mã văn bản  $C = \text{ZO BA TC ZI SN}$
- Cho  $k = \text{KEY}$ , giải mã văn bản  $C = \text{IK QB}$

## Mã Playfair (tt)

- Nhận xét:

- An toàn được nâng cao so hơn với bảng đơn, vì ta có tổng cộng  $26 \times 26 = 676$  cặp. Mỗi chữ có thể được mã bằng các chữ khác nhau, nên tần suất các chữ trên bản mã khác tần suất của các chữ cái trên văn bản tiếng Anh nói chung.
- Muốn sử dụng thống kê tần suất, cần phải có bảng tần suất của 676 cặp để thám mã (so với 26 của mã bảng đơn). Như vậy phải xem xét nhiều trường hợp hơn và tương ứng sẽ có thể có nhiều bản mã hơn cần lựa chọn. Do đó khó thám mã hơn mã trên bảng chữ đơn.
- Mã Playfair được sử dụng rộng rãi nhiều năm trong giới quân sự Mỹ và Anh trong chiến tranh thế giới thứ nhất. Nó có thể bị bẻ khoá nếu cho trước vài trăm chữ, vì bản mã vẫn còn chứa nhiều cấu trúc của bản rõ.

133


## Mã hoán vị (Permutation Cipher)

- Xáo trộn thứ tự của các chữ cái trong bản rõ
- Cách đơn giản: ghi bản rõ theo từng hàng, sau đó kết xuất bản mã theo cột.

Ví dụ: **attackpostponeduntilthisnoon**

- Viết lại thành ma trận  $4 \times 7$ :

a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
h	i	s	n	o	o	n



- Xuất theo cột:

**AODHTSUITTNSAPTNCIOKNLOPETN**

134

## Mã hoán vị (Permutation Cipher)

- Có thể hoán vị các cột trước khi kết xuất bản mã.
  - Ví dụ: với khóa là **MONARCH**, hoán vị các cột:

M O N A R C H		A C H M N O R
a t t a c k p		a k p a t t c
o s t p o n e	→	p n e o t s o
d u n t i l t		t l t d n u i
h i s n o o n		n o n h s i o

→ **A P T N C K N L O H P E T N M A O D H N T T N S O T S U I R C O I O**

135

## Mã hoán vị (Permutation Cipher)

- Hoán vị 2 lần (double transposition): sau khi hoán vị lần 1 → kết quả 1 → hoán vị lần 2
  - Ví dụ: với khóa là **MONARCH**, hoán vị 2 lần:

M O N A R C H		A C H M N O R	
a t t a c k p		a k p a t t c	
o s t p o n e	→	p n e o t s o	<b>A P T N C K N L O P E T N M A O D H N T T N S O T S U I C O I O</b>
d u n t i l t		t l t d n u i	
h i s n o o n		n o n h s i o	

M O N A R C H		A C H M N O R	
a p t n k n l		n n l a t p k	
o p e t n a o	→	t a o o e p n	<b>N T T C N A S I L O T O A O D S T E T I P P H U K N N O</b>
d h t t n s t		t s t d t h n	
s u i c o i o		c i o s i u o	

136

- ❑ Trong mã Affine, ta giới hạn xét các hàm mã có dạng:  
 $e(x) = ax + b \bmod 26$ ,  
 $a, b \in \mathbb{Z}_{26}$ . Các hàm này được gọi là các hàm Affine.
- ❑ Để việc giải mã có thể thực hiện được, yêu cầu cần thiết là hàm Affine phải là đơn ánh. Nghĩa là, với bất kỳ  $y \in \mathbb{Z}_{26}$ , ta muốn có đồng nhất thức như sau:  
 $ax + b \equiv y \pmod{26}$   
phải có nghiệm  $x$  duy nhất
- ❑ *Đồng dư thức  $ax \equiv y - b \pmod{26}$  chỉ có một nghiệm duy nhất  $x \in \mathbb{Z}_m$  với mọi  $b \in \mathbb{Z}_m$  khi và chỉ khi  $\text{UCLN}(a, m) = 1$ .*

137

- ❑ Giả sử  $P = C = \mathbb{Z}_{26}$ .

- *encryption:*  $e_k(x) = a \cdot x + b \bmod 26$ .
- *key:*  $k = (a, b)$  where  $a, b \in \mathbb{Z}_{26}$ .
- *decryption:*  $x = a^{-1}(y - b) \bmod 26$ .

$a$  và 26 là nguyên tố cùng nhau:  $\text{GCD}(a, 26) = 1$

138

- Mã Affine là một mã thay thế có dạng  
$$e(x) = ax + b \pmod{26}, \text{ trong đó } a, b \in \mathbb{Z}_{26}.$$
*Trường hợp  $a = 1$  là mã dịch chuyển.*
- Giải mã: Tìm  $x$ ?  
$$y = ax + b \pmod{26}$$
$$ax = y - b \pmod{26}$$
$$x = a^{-1}(y - b) \pmod{26}.$$
- Vấn đề: Cần tính được  $a^{-1}$ .  
Để có  $a^{-1}$ ,  $\text{GCD}(a, 26) = 1$ .  
Tính  $a^{-1}$ : Dùng thuật toán Euclide mở rộng.

139

Công thức tổng quát:  $a^{-1} \pmod{N}$

-Giá trị điền sẵn:

$$X_1 = N; B_1 = 0$$

$$X_2 = a; B_2 = 1$$

-Giá trị điền tính toán:

$$X_i = X_{i-2} \pmod{X_{i-1}}$$

$$Y_i = X_{i-1} \text{ div } X_i \text{ (chia lấy nguyên)}$$

$$B_i = B_{i-2} - (B_{i-1} * Y_{i-1})$$

Dừng khi  $X_i = 1$ , và kết quả là  $a^{-1} = B_i$  (Nếu âm  $a^{-1} = B_i + N$ )

140

## Thuật toán Euclide mở rộng

Công thức tổng quát:  $a^{-1} \bmod N$

- Giá trị điền sẵn:

$$X_1 = N; B_1 = 0$$

$$X_2 = a; B_2 = 1$$

- Giá trị điền tính toán:

$$X_i = X_{i-2} \bmod X_{i-1}$$

$$Y_i = X_{i-1} \div X_i \text{ (chia lấy nguyên)}$$

$$B_i = B_{i-2} - (B_{i-1} * Y_{i-1})$$

Dừng khi  $X_i = 1$ , và kết quả là  $a^{-1} = B_i$  (Nếu âm  $a^{-1} = B_i + N$ )

	X	B	Y
1	Giá trị N	0	
2	Giá trị a	1	$Y_2$
i	$X_i$	$B_i$	$Y_i$

141

## Thuật toán Euclide mở rộng

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

VD: cho  $K(7,3)$ ,  $N=26$ , giải mã AXG

$$\text{UCNL}(7,26) = 1$$

Tính  $7^{-1} \bmod 26$  ?

	X	B	Y
1	26	0	
2	7	1	3
3	5	-3	1
4	2	4	2
5	1	-11	2

$$Y_2 = X_{2-1} \div X_2 = X_1 \div X_2 = 26 \div 7 = 3$$

$$X_3 = X_{3-2} \bmod X_{3-1} = X_1 \bmod X_2 = 26 \bmod 7 = 5$$

$$Y_3 = X_{3-1} \div X_3 = X_2 \div X_3 = 7 \div 5 = 1$$

$$B_3 = B_{3-2} - (B_{3-1} * Y_{3-1}) = B_1 - (B_2 * Y_2) = 0 - (1 * 3) = -3$$

$$X_4 = X_2 \bmod X_3 = 7 \bmod 5 = 2$$

$$Y_4 = X_3 \div X_4 = 5 \div 2 = 2$$

$$B_4 = B_2 - (B_3 * Y_3) = 1 - (-3 * 1) = 4$$

$$X_5 = X_3 \bmod X_4 = 5 \bmod 2 = 1$$

$$Y_5 = X_4 \div X_5 = 2 \div 1 = 2$$

$$B_5 = B_3 - (B_4 * Y_4) = -3 - (4 * 2) = -11$$

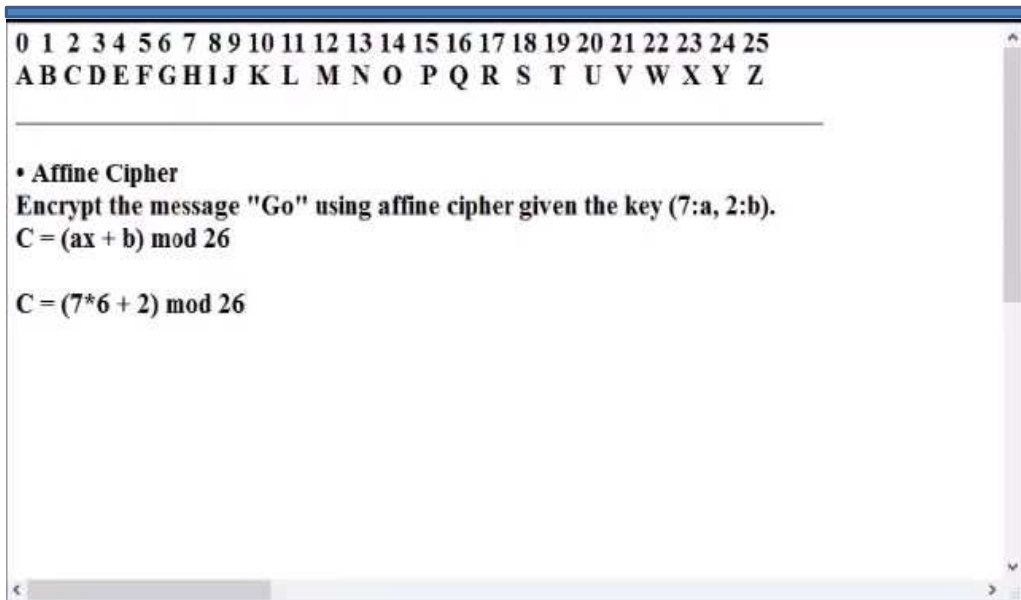
$$\Rightarrow [-11 + 26] \bmod 26 = 15$$

142



- ☐ Tính  $9^{-1} \bmod 26$  bằng Euclide mở rộng
- ☐ Tính  $13^{-1} \bmod 26$  bằng Euclide mở rộng
- ☐ Tính  $15^{-1} \bmod 26$  bằng Euclide mở rộng
- ☐ Tính  $23^{-1} \bmod 26$  bằng Euclide mở rộng

143



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25  
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

---

• Affine Cipher  
Encrypt the message "Go" using affine cipher given the key (7:a, 2:b).  
 $C = (ax + b) \bmod 26$   
 $C = (7*6 + 2) \bmod 26$

144

## Hệ mã Affine

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

**Mã hóa văn bản: “HELLO WORLD” với khóa là (17, 6)**

- Trong bảng mã ABC..XYZ, ta có  $m = 26$
- Văn bản gốc được chuyển thành dãy số  $[7, 4, 11, 11, 14, 22, 14, 17, 11, 3]$
- Với từng số  $x$  trong dãy số trên, áp dụng hàm mã

hóa  $E(x) = (17x + 6) \bmod 26$ , ta được dãy số  $[21, 22, 11, 11, 10, 16, 10, 11, 9, 5]$

- Chuyển dãy số về dạng ABC, ta có bản mã: VWLLK QKJLF

145

## Hệ mã Affine

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

**Giải mã văn bản: “VWLLK QKJLF” với khóa là (17, 6)**

- Trong bảng mã ABC..XYZ, ta có  $m = 26$
- Văn bản mã được chuyển thành dãy số  $C1 = [21, 22, 11, 11, 10, 16, 10, 11, 9, 5]$
- Nghịch đảo của 17 theo module 26 là 23, ta có  $a^{-1} = 23$
- Với từng số  $x$  trong dãy số  $C1$ , áp dụng hàm giải mã  $D(x) = a^{-1}(x - b) \bmod m = 23(x - 6) \bmod 26$ , ta được dãy số  $[7, 4, 11, 11, 14, 22, 14, 17, 11, 3]$
- Chuyển dãy số này về dạng ABC, ta được văn bản gốc: HELLO WORLD

146

❖ Hàm mã  $y = 5x + 3 \pmod{26}$

- Cho bản rõ P= DAIHOCTMO. Với  $a = 5$ ,  $b = 3$ . Hãy tìm bản mã theo thuật mã Affine ?
- Cho bản rõ “TK” khóa  $k = (23, 7)$ . Tìm bản mã ?
- Cho bản rõ “EXIT” khóa  $k = (7, 3)$ . Tìm bản mã ?
- Cho bản mã “IZB” khóa  $k = (19, 3)$ . Tìm bản rõ ?
- Giải mã “HUAXTGO” khóa  $k = (5, 6)$ . Tìm bản rõ ?

147

Phương pháp Hill (1929)

Tác giả: Lester S. Hill

Ý tưởng chính:

Sử dụng  $m$  tổ hợp tuyến tính của  $m$  ký tự trong plaintext để tạo ra  $m$  ký tự trong ciphertext

Ví dụ:

$$\begin{aligned} y_1 &= 11x_1 + 3x_2 \\ y_2 &= 8x_1 + 7x_2. \end{aligned} \quad (y_1, y_2) = (x_1, x_2) \begin{pmatrix} 11 & 3 \\ 8 & 7 \end{pmatrix}$$

148

## Mã hóa Hill

Chọn số nguyên dương  $m$ . Định nghĩa:

$P = C = (\mathbb{Z}_n)^m$  và  $K$  là tập hợp các ma trận  $m \times m$  khả nghịch

Với mỗi khóa  $k = \begin{pmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,m} \\ k_{2,1} & \cdots & \cdots & k_{2,m} \\ \vdots & \vdots & & \vdots \\ k_{m,1} & k_{m,2} & \cdots & k_{m,m} \end{pmatrix} \in K$ , định nghĩa:

$$e_k(x) = xk = (x_1, x_2, \dots, x_m) \begin{pmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,m} \\ k_{2,1} & \cdots & \cdots & k_{2,m} \\ \vdots & \vdots & & \vdots \\ k_{m,1} & k_{m,2} & \cdots & k_{m,m} \end{pmatrix} \text{ với } x = (x_1, x_2, \dots, x_m) \in P$$

và  $d_k(y) = yk^{-1}$  với  $y \in C$ .

Mọi phép toán số học đều được thực hiện trên  $\mathbb{Z}_n$ .

149

## Mã hóa Hill

Ví dụ: cho hệ mã Hill có  $M = 2$  (khóa là các ma trận vuông cấp 2) và bảng chữ cái là bảng chữ cái tiếng Anh, tức là  $N = 26$ . Cho khóa

$$K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$$

Hãy mã hóa bản rõ  $P = \text{"HELP"}$  và thực hiện giải mã ngược lại bản mã thu được sau khi mã hóa.

150

Để mã hóa chúng ta chia chuỗi bản rõ thành hai vector hàng 2 chiều “HE” (7 4) và “LP” (11 15) và tiến hành mã hóa lần lượt.

$$\text{Với } P_1 = (7 \ 4) \text{ ta có } C_1 = P_1 * K = (7 \ 4) \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} = (3 \ 15) = (D \ P)$$

$$\text{Với } P_2 = (11 \ 15) \text{ ta có } C_2 = P_2 * K = (11 \ 15) \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} = (11 \ 4) = (L \ E)$$

Vậy bản mã thu được là C = “DPLE”.

151

$$AB = \begin{bmatrix} 1 & 4 \\ 5 & 2 \end{bmatrix} \begin{bmatrix} 3 & -1 \\ 4 & 0 \end{bmatrix} = \begin{bmatrix} 19 & -1 \\ 23 & -5 \end{bmatrix}$$

$$BA = \begin{bmatrix} 3 & -1 \\ 4 & 0 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 5 & 2 \end{bmatrix} = \begin{bmatrix} -2 & 10 \\ 4 & 16 \end{bmatrix}$$

152

- Để giải mã ta tính khóa giải mã là ma trận nghịch đảo của ma trận khóa trên  $Z_{26}$  theo công thức sau:

Với  $K = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$  và  $\det(K) = (k_{11} \cdot k_{22} - k_{21} \cdot k_{12}) \bmod N$  là một phần tử có phần tử

nghịch đảo trên  $Z_N$  (ký hiệu là  $\det(K)^{-1}$ ) thì khóa giải mã sẽ là

$$K^{-1} = \det(K)^{-1} \cdot \begin{pmatrix} k_{22} & -k_{12} \\ -k_{21} & k_{11} \end{pmatrix}$$

Áp dụng vào trường hợp trên ta có  $\det(K) = (15 - 6) \bmod 26 = 9$ .  $\text{GCD}(9, 26) = 1$  nên

- Áp dụng thuật toán Euclid mở rộng ta được:  $\det(K)^{-1} = 3$ . Vậy  $K^{-1} = 3 \cdot \begin{pmatrix} 5 & 23 \\ 24 & 3 \end{pmatrix} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}$ .

153

$$\text{Giải mã } C = \text{"DP"} = \begin{pmatrix} 3 & 15 \end{pmatrix}, P = C \cdot K^{-1} = \begin{pmatrix} 3 & 15 \end{pmatrix} \cdot \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} = \begin{pmatrix} 3 & 15 \end{pmatrix} = \text{"HE"}.$$

- Tương tự ta giải mã cặp  $C = \text{"DP"}$  ta có được kết quả bản rõ  $P = \text{"LP"}$

Chú ý là trong ví dụ trên chúng ta sử dụng khóa  $K$  có kích thước nhỏ nên dễ dàng tìm được khóa để giải mã còn trong trường hợp tổng quát điều này là không dễ dàng.

154

## Mã hóa Hill (minh họa)

$$\text{Det}(K) = (3*5 - 2*3) \bmod 26 = 9 \bmod 26 = 9$$

$$\text{Det}(K)^{-1} = 3 \quad \text{Dùng Euclid mở rộng để tính được từ } \text{Det}(K)=9$$

$$K^{-1} = 3 * \begin{pmatrix} 5 & -3 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} 15 & -9 \\ -6 & 9 \end{pmatrix} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}$$

155

## Mã hóa Hill (minh họa)

$$P_1 = C_1 * K^{-1} = (3, 15) \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} = (7, 4) = \text{HE}$$

$$P_2 = C_2 * K^{-1} = (11, 4) \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} = (11, 15) = \text{LP}$$

Kết quả : P = HELP

156

## Mã hóa Hill – Bài tập

1. Cho bản rõ “so” khóa k là:

7	2
3	3

Hãy mã hóa bản rõ với khóa k theo hệ mã Hill. Biết hàm mã  $y = xk$

2. Cho bản rõ “lo” khóa k là:

8	11
1	2

Hãy mã hóa bản rõ với khóa k theo hệ mã Hill. Biết hàm mã  $y = xk$

3. Cho bản mã “KS” khóa k là ma trận cấp 2 sau:

3	4
1	3

Hãy giải mã bản mã với khóa k theo hệ mã Hill tìm bản rõ nào . Biết hàm mã hóa  $y = kx$

157



## Các hệ mật đối xứng hiện đại

- Mã hóa dữ liệu nhị phân/ mã hóa khối, bao gồm:
  - Mã dòng (Stream Cipher)
    - A5/1
    - RC4
  - Mã khối (Block Cipher)
    - SPN
    - Feistel
    - DES

158



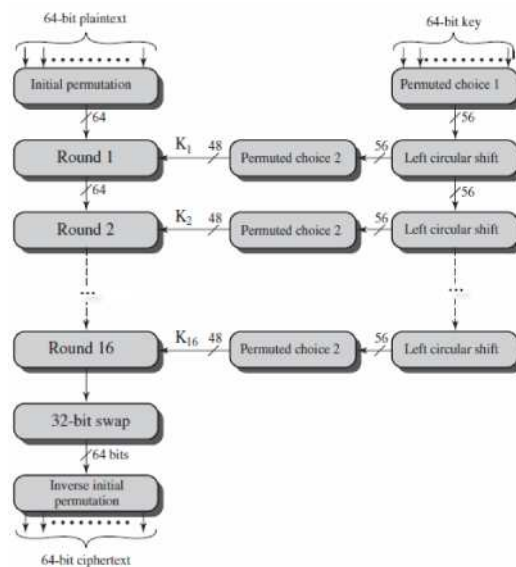
## Hệ mật DES (Data Encryption Standards)

- Là mã khối ra đời năm 1977 bởi NBS – văn phòng chuẩn Quốc gia Hoa kỳ (bây giờ là NIST - Viện chuẩn và công nghệ Quốc gia).
- DES là thuật toán mã hóa khối, độ dài mỗi khối là 64 bit .
- Nguyên lý:
  - Sử dụng một khóa K tạo ra n khóa con  $K_1, K_2, \dots, K_n$
  - Hoán vị dữ liệu (Initial Permutation)
  - Thực hiện n vòng lặp, ở mỗi vòng lặp
    - Dữ liệu được chia thành hai phần
    - Áp dụng phép toán thay thế lên một phần, phần còn lại giữ nguyên
    - Hoán vị 2 phần cho nhau (trái  $\leftrightarrow$  phải)
  - Hoán vị dữ liệu (Final Permutation)

159

## Hệ mật DES (tt)

- Thuật toán DES: gồm ba phần
  - Các hoán vị khởi tạo và hoán vị kết thúc.
  - Các vòng Feistel
  - Thuật toán sinh khóa con.



General Depiction of DES Encryption Algorithm

160

- Các bước mã hóa: bản rõ  $M$  được biểu diễn thành dãy 64 bit, tiến hành 3 bước:
  - 1. Tạo dãy 64 bit  $X$  bằng cách hoán vị  $M$  theo bảng hoán vị IP (Initial Permutation):  $X = IP(M) = L_0R_0$  (32 bit trái-32 bit phải của  $X$ )
  - 2. Thực hiện 16 vòng lặp từ 64 bit thu được và 56 bit của khóa  $K$  (chỉ sử dụng 48 bit), 64 bit thu được qua mỗi vòng lặp sẽ là đầu vào của vòng lặp tiếp theo.
    - $L_i = R_{i-1}$
    - $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$
    - $\oplus$  biểu diễn phép toán XOR trên hai dãy bit  $K_1, K_2, \dots, K_{16}$  là các dãy 48 bit phát sinh từ khóa  $K$  ( $K_i$  có được do hoán vị các bit trong khóa  $K$ )
  - 3. Áp dụng hoán vị ngược  $IP^{-1}$  đối với dãy bit  $L_{16}R_{16}$  thu được 64 bit  $Y = IP^{-1}(L_{16}R_{16})$

161

- **Hoán vị khởi tạo:**
  - Ta đánh số các bit của khối 64 bit ( $M$ ) theo thứ tự từ trái sang phải là 1, 2, 3, ..., 63, 64
  - Hoán vị khởi tạo sẽ hoán đổi các bit theo bảng IP  
 $X = IP(M) = L_0R_0$

Initial Permutation (IP)							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	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

162

- **Hoán vị khởi tạo:**

– Ví dụ:

$M_1$	$M_2$	$M_3$	$M_4$	$M_5$	$M_6$	$M_7$	$M_8$		$M_{58}$	$M_{50}$	$M_{42}$	$M_{34}$	$M_{26}$	$M_{18}$	$M_{10}$	$M_2$
$M_9$	$M_{10}$	$M_{11}$	$M_{12}$	$M_{13}$	$M_{14}$	$M_{15}$	$M_{16}$		$M_{60}$	$M_{52}$	$M_{44}$	$M_{36}$	$M_{28}$	$M_{20}$	$M_{12}$	$M_4$
$M_{17}$	$M_{18}$	$M_{19}$	$M_{20}$	$M_{21}$	$M_{22}$	$M_{23}$	$M_{24}$		$M_{62}$	$M_{54}$	$M_{46}$	$M_{38}$	$M_{30}$	$M_{22}$	$M_{14}$	$M_6$
$M_{25}$	$M_{26}$	$M_{27}$	$M_{28}$	$M_{29}$	$M_{30}$	$M_{31}$	$M_{32}$		$M_{64}$	$M_{56}$	$M_{48}$	$M_{40}$	$M_{32}$	$M_{24}$	$M_{16}$	$M_8$
$M_{33}$	$M_{34}$	$M_{35}$	$M_{36}$	$M_{37}$	$M_{38}$	$M_{39}$	$M_{40}$		$M_{57}$	$M_{49}$	$M_{41}$	$M_{33}$	$M_{25}$	$M_{17}$	$M_9$	$M_1$
$M_{41}$	$M_{42}$	$M_{43}$	$M_{44}$	$M_{45}$	$M_{46}$	$M_{47}$	$M_{48}$		$M_{59}$	$M_{51}$	$M_{43}$	$M_{35}$	$M_{27}$	$M_{19}$	$M_{11}$	$M_3$
$M_{49}$	$M_{50}$	$M_{51}$	$M_{52}$	$M_{53}$	$M_{54}$	$M_{55}$	$M_{56}$		$M_{61}$	$M_{53}$	$M_{45}$	$M_{37}$	$M_{29}$	$M_{21}$	$M_{13}$	$M_5$
$M_{57}$	$M_{58}$	$M_{59}$	$M_{60}$	$M_{61}$	$M_{62}$	$M_{63}$	$M_{64}$		$M_{63}$	$M_{55}$	$M_{47}$	$M_{39}$	$M_{31}$	$M_{23}$	$M_{15}$	$M_7$

163

- **Hoán vị kết thúc:**

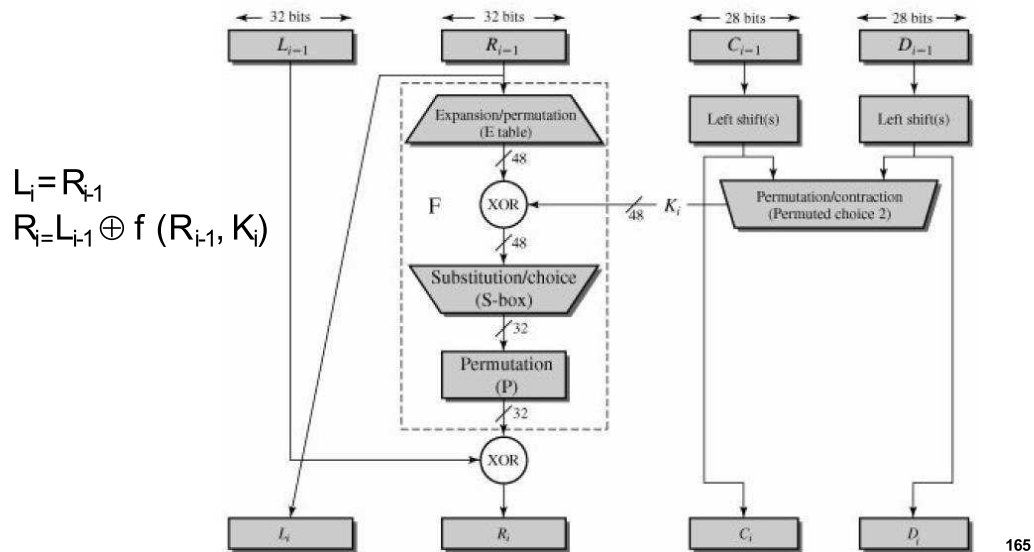
– Là hoán vị nghịch đảo của hoán vị khởi tạo hoán đổi các bit theo quy tắc sau:  $Y = IP^{-1}(L_{16}R_{16})$

Inverse Initial Permutation ( $IP^{-1}$ )							
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

164

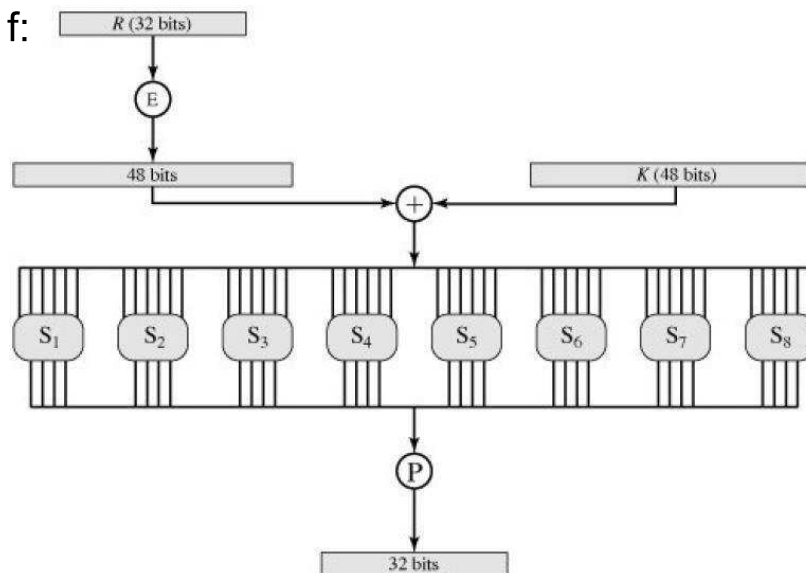
## Hệ mật DES (tt)

### • Chi tiết tại mỗi vòng:



## Hệ mật DES (tt)

### • Hàm f:



- Hàm  $f$ : đối số đầu là  $R_{i-1}$  (32 bit) đối số thứ hai là  $K_i$  (48 bit) và tạo ra dãy có độ dài 32 bit, thực hiện theo các bước sau:
  - $R_{i-1}$  sẽ được “mở rộng” thành dãy có độ dài 48 bit tương ứng với hàm mở rộng  $E$  cố định.  $E(R_i)$  bao gồm 32 bit từ  $R_i$ , được hoán vị theo một cách thức xác định, với 16 bit được tạo ra 2 lần.
  - Tính  $E(R_{i-1}) \oplus K_i$  kết quả được một khối có độ dài 48 bit. Khối này sẽ được chia làm 8 khối  $B=B_1B_2B_3B_4B_5B_6B_7B_8$ . Mỗi khối này có độ dài là 6 bit.

167

- $E(R_i)$

Expansion Permutation (E)						
	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

168

4. Bước kế tiếp là cho các khối Bi đi qua hộp Si sẽ biến một khối có độ dài 6 bit thành một khối Ci có độ dài 4 bit.
- Mỗi hộp S-box là một bảng gồm 4 hàng và 16 cột được đánh số từ 0. Như vậy mỗi hộp S có hàng 0,1,2,3. Cột 0,1,2,...,15. Mỗi phần tử của hộp là một số 4 bit. Sáu bit vào hộp S sẽ xác định số hàng và số cột để tìm kết quả ra.
  - Mỗi khối Bi có 6 bit kí hiệu là b1, b2, b3, b4, b5 và b6. Bit b1 và b6 được kết hợp thành một số 2 bit, nhận giá trị từ 0 đến 3, tương ứng với một hàng trong bảng S. Bốn bit ở giữa, từ b2 tới b5, được kết hợp thành một số 4 bit, nhận giá trị từ 0 đến 15, tương ứng với một cột trong bảng S.

Hộp S1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Hộp S2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

## Hệ mật DES (tt)

Hộp S3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

Hộp S4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

171

## Hệ mật DES (tt)

Hộp S5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Hộp S6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

172

## Hệ mật DES (tt)

Hộp S7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

Hộp S8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

173

## Hệ mật DES (tt)

- Ví dụ: Ta có  $B1=011000$  thì  $b_1b_6=00$  (xác định  $r=0$ ),  $b_2b_3b_4b_5=1100$  (xác định  $c=12$ ), từ đó ta tìm được phần tử ở vị trí  $(0,12) \rightarrow S1(B1)=0101$  (tương ứng với số 5).

$b_1b_6=00$  →

$b_2b_3b_4b_5=1100$  ↓

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Hộp S1

174



## Hệ mật DES (tt)

4. Chuỗi bit  $C = C_1C_2C_3C_4C_5C_6C_7C_8$  có độ dài 32 bit được hoán vị tương ứng với hoán vị cố định P. Kết quả có  $P(C) = f(R_i, K_i)$ .

Hoán vị P

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

175

## Hệ mật DES (tt)

### • Sinh khóa:

- Khóa K là dãy 64 bits trong đó có 56 bits làm khóa và 8 bits dùng để kiểm tra lỗi (Kiểm tra chẵn lẻ)
- Các bit nằm ở vị trí 8, 16, 24 ... 64 là các bit dùng để kiểm tra chẵn lẻ
- Cho một khóa K 64 bits, ta sẽ bỏ các bit kiểm tra được 56 bits khóa.
- Cho 56 bit này hoán vị theo bảng hoán vị PC-1.
- Ta có:  $PC-1(K) = C_0D_0$ 
  - Trong đó:  $C_0$  chứa 28 bit bên trái
  - $D_0$  chứa 28 bit bên phải

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

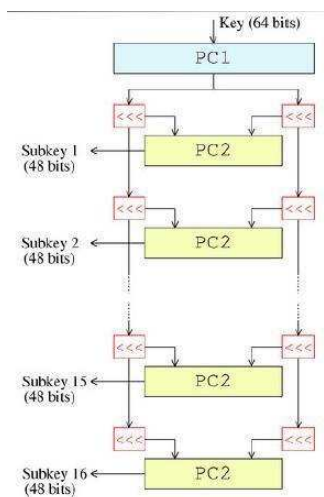
Chọn 56 bit  
(bỏ bit 8, 16, 24, 32,  
40, 48, 56, 64)

176

- Cho  $i$  chạy từ 1 đến 16, tính:
  - $C_i = LSi(C_{i-1})$
  - $D_i = LSi(D_{i-1})$
  - $K_i = PC-2(C_i D_i)$
- Với  $LSi$  là dịch chuyển vòng sang trái một hay hai vị trí tùy thuộc vào giá trị của  $i$ :
  - 1 vị trí nếu  $i = 1, 2, 9, 16$
  - 2 vị trí trong các trường hợp còn lại

Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

177



178

## Hệ mật DES (tt)

- $K[i] = PC-2(C[i]D[i])$ 
  - PC2: Bảng hoán vị dãy  $CiDi$  thành 56 bit thành 48 bit

PC-2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Chọn 48 bit  
(bỏ bit 9, 18, 22, 25,  
35, 38, 43, 54)

179

## Hệ mật DES (tt)

- Tóm tắt giải thuật:

### Tạo 16 khóa con

```

C[0]D[0] = PC-1(KEY)
for i = 1 to 16
    C[i] = LeftShift[i](C[i-1])
    D[i] = LeftShift[i](D[i-1])
end for
K[i] = PC-2(C[i]D[i])
    
```

### M. hóa khối dữ

liệu  $L[0]R[0] = IP(\text{plain block})$

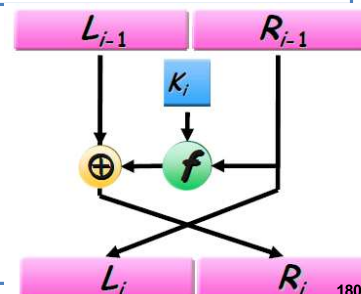
for  $i=1$  to 16

$L[i] = R[i-1]$

$R[i] = L[i-1] \text{ XOR } F(R[i-1], K[i])$

end for

cipher block =  $FP(R[16]L[16])$



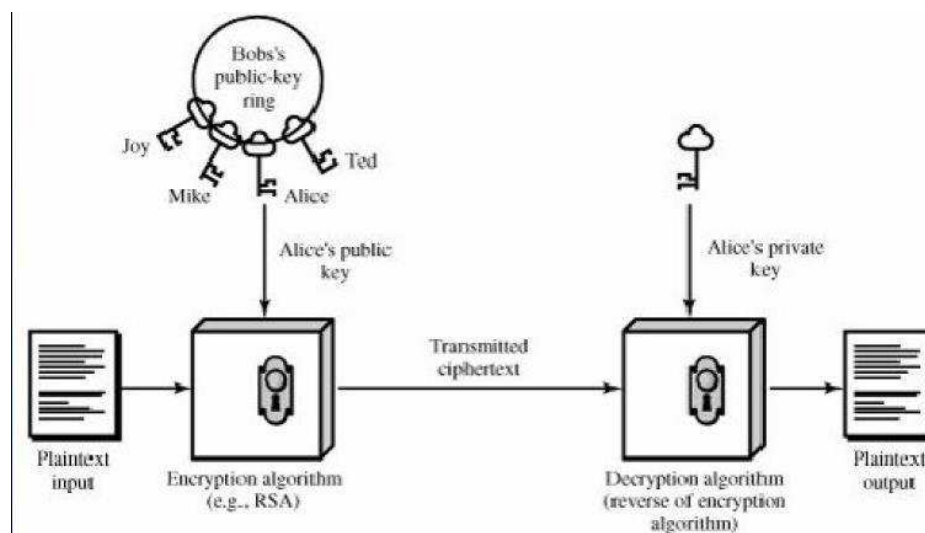
180

## 4.3 Hệ mật bất đối xứng

- Còn gọi là hệ mật mã khóa công khai
- Dùng một khoá để thực hiện mã hoá sau đó dùng một khoá khác để giải mã, nghĩa là khoá để mã hoá và giải mã là khác nhau.
- Các khoá này tạo nên từng cặp chuyển đổi ngược nhau và các khoá không thể suy được từ khoá kia.
- Khoá dùng để mã hoá có thể công khai nhưng khoá dùng để giải mã phải giữ bí mật.

181

## 4.3 Hệ mật bất đối xứng



182

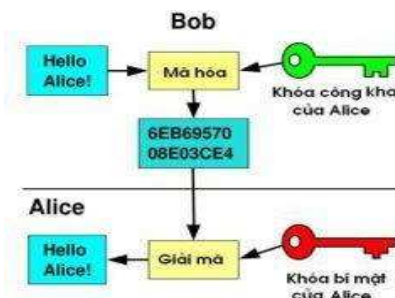
### 4.3.1 RSA (Rivest – Shamir – Adleman)

- Được phát triển bởi Ron Rivest, Adi Shamir và Adleman tại học viện MIT vào năm 1977
- Sử dụng biểu thức hàm mũ
- Văn bản rõ được mã hóa ở dạng khối, kích cỡ của khối phải nhỏ hơn hoặc bằng  $\log_2(n)$
- Trên thực tế, kích thước khối là  $i$  bit, với  $2^i < n \leq 2^{i+1}$
- Mã hóa và giải mã được thực hiện với một số khối rõ  $M$  (plaintext) và khối mã  $C$  (ciphertext):
  - $C = M^e \bmod n$
  - $M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

183

### RSA (tt)

- Kịch bản: Bob muốn gửi tài liệu mật cho Alice.
  - Alice tạo ra một khóa bí mật (private key) và từ khóa bí mật này tính ra khóa công khai (public key) (với một thủ tục không phức tạp).
  - Alice gửi cho Bob khóa công khai của mình
  - Bob mã hóa văn bản bằng khóa công cộng của Alice và gửi bản tin mã cho Alice.
  - Alice giải mã tài liệu Bob gửi bằng khóa bí mật của mình.



184

- Thuật toán xác định khóa:

### Key Generation

Select $p, q$	$p$ and $q$ both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p - 1)(q - 1)$	
Select integer $e$	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate $d$	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

185

- Mã hóa và giải mã

### Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

### Decryption

Ciphertext:	$C$
Plaintext:	$M = C^d \pmod{n}$

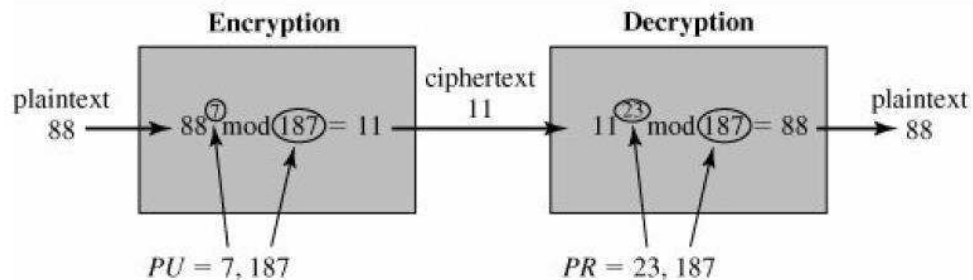
186

### • Các yêu cầu:

- Cả người gửi và người nhận đều phải biết giá trị của  $n$
- Người gửi chỉ biết  $e$ , người nhận chỉ biết  $d$
- Phải có khả năng tìm được giá trị của  $e$ ,  $d$ ,  $n$  sao cho  $M^{ed} \bmod n = M$ , với  $M < n$
- Phải dễ dàng tính toán được  $M^e \bmod n$  và  $C^d \bmod n$  cho tất cả các giá trị của  $M < n$
- Không thể xác định được  $d$  khi biết  $e$  và  $n$
- $p$  và  $q$  cần rất lớn để không phân tích được  $n = pq$

187

### • Ví dụ 1 (đã xác định khóa)



Với:

$M = 88$

$n = 187$

$e = 7$

$d = 23$

188

- Với  $M = 88$ ,  $n = 187$ ,  $e = 7$ ,  $d = 23$
- Để mã hóa cần tính được  $C = 88^7 \bmod 187$ .

$$88^7 \bmod 187 = [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$$

$$88^1 \bmod 187 = 88$$

$$88^2 \bmod 187 = 7744 \bmod 187 = 77$$

$$88^4 \bmod 187 = 59.969.536 \bmod 187 = 132$$

$$88^7 \bmod 187 = (88 \times 77 \times 132) \bmod 187 = 894.432 \bmod 187 = 11$$

- Để giải mã, cần tính  $M = 11^{23} \bmod 187$

$$11^{23} \bmod 187 = [(11^1 \bmod 187) \times (11^2 \bmod 187) \times (11^4 \bmod 187) \times (11^8 \bmod 187) \times (11^8 \bmod 187)] \bmod 187$$

$$11^1 \bmod 187 = 11$$

$$11^2 \bmod 187 = 121$$

$$11^4 \bmod 187 = 14.641 \bmod 187 = 55$$

$$11^8 \bmod 187 = 214.358.881 \bmod 187 = 33$$

$$11^{23} \bmod 187 = (11 \times 121 \times 55 \times 33 \times 33) \bmod 187 = 79.720.245 \bmod 187 = 88$$

189

- Ví dụ 2 (có chọn khóa):
  - Chọn  $p = 11$ ,  $q = 3 \rightarrow N = pq = 33$
  - $n = (p-1)(q-1) = 20$
  - Chọn  $e = 3$  là nguyên tố cùng nhau với  $n$
  - Tìm nghịch đảo của  $e$  trong phép mod  $n$  được  $d = 7$
  - Khóa công khai  $K_U = (e, N) = (3, 33)$ .
  - Khóa bí mật  $K_R = (d, N) = (7, 33)$

190

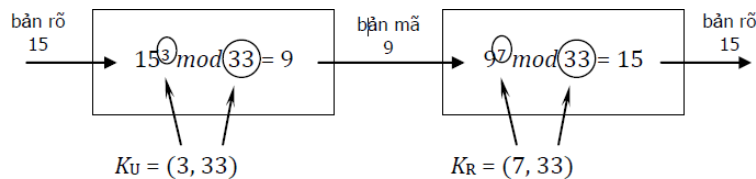


- Mã hóa bản rõ  $M = 15$ :

$$C = M^e \bmod N = 15^3 \bmod 33 = 9 \quad (\text{vì } 15^3 = 3375 = 102 \times 33 + 9)$$

- Giải mã với bản mã  $C = 9$ :

$$\bar{M} = C^d \bmod N = 9^7 \bmod 33 = 15 = M \quad (\text{vì } 9^7 = 4.782.696 = 144.938 \times 33 + 15)$$



191

- ☐ Người A chọn các thông số  $p = 17$ ,  $q = 3$ ,  $e = 5$ . Hỏi khóa riêng của A là gì ?
- ☐ Người A chọn các thông số  $p = 23$ ,  $q = 17$ ,  $e = 37$ . Hỏi cặp khóa riêng của A theo thuật mã RSA là gì?
- ☐ Cho bản mã  $y = 18$ , khóa công khai  $n = 221$ ,  $e = 91$ . Giải mã với khóa trên theo hệ mã RSA tìm bản rõ ?
- ☐ Người A chọn các thông số  $p = 31$ ,  $q = 37$ ,  $e = 397$ . Khi giải mã bản mã với  $C = 509$  theo thuật mã RSA chúng ta sẽ thu được bản rõ nào ?

192

## 4.3.2 Thuật giải Diffie-Hellman

- Cho phép hai người dùng trao đổi khóa bí mật dùng chung trên mạng công cộng, sau đó có thể sử dụng để mã hóa các thông điệp
- Thuật toán tập trung vào giới hạn việc trao đổi các giá trị bí mật, xây dựng dựa trên bài toán khó sử dụng logarit rời rạc

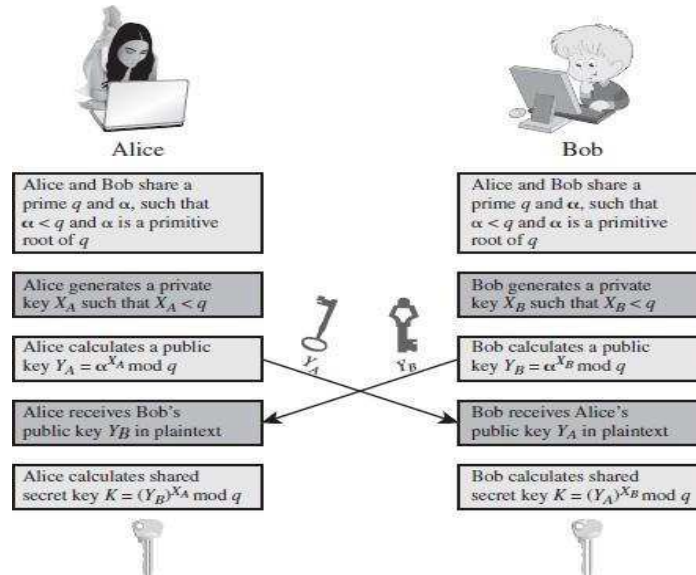
193

## Diffie-Hellman (tt)

- Giao thức trao đổi khóa giữa A và B
  - A và B thống nhất chung một số nguyên tố  $q$  và một phần tử sinh  $\alpha$
  - A chọn ngẫu nhiên một số  $X_A \in (1, 2, \dots, q-1)$  rồi gửi cho B kết quả  $Y_A = \alpha^{X_A} \bmod q$
  - B chọn ngẫu nhiên một số  $X_B \in (1, 2, \dots, q-1)$  rồi gửi cho A kết quả  $Y_B = \alpha^{X_B} \bmod q$
  - A tính khóa bí mật:  $K = (\alpha^{X_B})^{X_A} \bmod q = \alpha^{X_A X_B} \bmod q$
  - B tính khóa bí mật:  $K = (\alpha^{X_A})^{X_B} \bmod q = \alpha^{X_A X_B} \bmod q$

194

## Diffie-Hellman (tt)



195

## Diffie-Hellman (tt)

Định lý Ôle phát biểu như sau:

$a \in \mathbb{Z}_N^* = \mathbb{Z}_N - \{0\}$  và  $\gcd(a, N) = 1$  ta có  
 $a^{\phi(N)} \equiv 1 \pmod{N}$ . Có nghĩa  $a^{\phi(N)}$  chính là giá trị  
 nghịch đảo của  $a$  trên  $\mathbb{Z}_N$ .

Định lý Fermat nhỏ (Trường hợp riêng định lý Ôle):

Nếu  $P$  là một số nguyên tố thì

$$a \in \mathbb{Z}_P^* \text{ ta có } a^{P-1} \equiv 1 \pmod{P}$$

196

Nếu bậc của  $a \in \mathbb{Z}_N^*$  bằng  $\varphi(N)$  thì **a được gọi là phần tử sinh** hay phần tử nguyên thủy của tập  $\mathbb{Z}_N^*$  và nếu tập  $\mathbb{Z}_N^*$  chỉ có một phần tử sinh thì nó được gọi là một cyclic.

Ví dụ:  $N=3$ ,  $a=2$ ; ( $N \in \mathbb{P}$ )

$$\varphi(N) = (N-1) = 2$$

$$\text{Ord}(a) = t = 2 \quad \text{vì } a^t \bmod N = 2^2 \bmod 3 = 1$$

$a = \varphi(N) = 2$  vậy 2 là phần tử nguyên thủy của  $\mathbb{Z}_{(2)}^*$

197

- Ví dụ

- A và B chọn số nguyên tố chung  $q=353$  và phần tử sinh  $\alpha=3$
- A chọn ngẫu nhiên  $X_A = 97$  rồi gửi cho B giá trị kết quả của  $3^{97} \bmod 353 = 40$
- B chọn  $X_B = 233$  rồi gửi cho A giá trị kết quả của  $3^{233} \bmod 353 = 248$
- Cả A và B đều tính được  $K = 248^{97} \bmod 353 = 160 = 40^{233} \bmod 353$

198

- Ví dụ 2:

- 1. A và B thỏa thuận sử dụng chung 2 số  $p = 17$  và  $g = 3$ .
- 2. A chọn 1 số nguyên bí mật  $a = 2$  và gửi cho B giá trị  $A = g^a \bmod p$   
Ta có :  $A = 3^2 \bmod 17 = 9$
- 3. B chọn 1 số nguyên bí mật  $b = 5$  và gửi cho A giá trị  $B = g^b \bmod p$   
Ta có :  $B = 3^5 \bmod 17 = 5$
- 4. A tính  $s = B^a \bmod p = 5^2 \bmod 17 = 8$
- 5. B tính  $s = A^b \bmod p = 9^5 \bmod 17 = 8$   
Ta có : Số bí mật của A và B là 8

199

- ☐ Cho A,B chọn 2 số nguyên tố chung là  $g = 10$  ,  $p = 541$ , với  $a=5$ ,  $b=7$  . Tính khóa công khai, khóa riêng của người gửi và người nhận A,B.
- ☐ Cho A,B chọn 2 số nguyên tố chung là  $g=2$  ,  $p = 997$ ,  $a=11$ ,  $b= 13$ . Tính khóa công khai, khóa riêng của người gửi và người nhận A, B.
- ☐ Cho A,B chọn 2 số nguyên tố chung là  $g=2$  ,  $p = 23$ ,  $a=5$ ,  $b= 13$ . Tính khóa công khai, khóa riêng của người gửi và người nhận A, B.

200

## 4.4 Hàm băm một chiều (One Way Hash function)

- Khái niệm
- SHA-1 (Secure Hash Algorithm)
- SHA-2
- MD5
- Một số hàm băm khác.

201

### 4.4.1 Khái niệm hàm băm

- Hàm băm nhận một chuỗi ở đầu vào, cắt nó ra nhiều phần, trộn lẫn chúng để tạo ra chuỗi mới có chiều dài ngắn.
- Các hàm băm (H) tạo ra bản nhận dạng (fingerprint) cho một tập tin, thông điệp hay một khối dữ liệu truyền đi nhằm kiểm tra tính toàn vẹn.
- Hàm băm thỏa các tiêu chuẩn:
  - Có thuộc tính một chiều
  - Có thuộc tính duy nhấtĐược gọi là hàm băm mật mã (Cryptographic Hash Function – CHF)

202

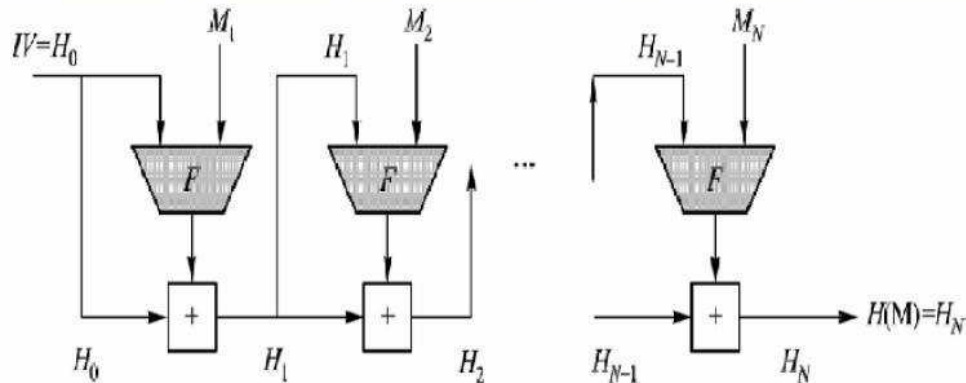
- Các đặc điểm
  - H có thể được áp dụng trên khối dữ liệu có độ dài bất kỳ
  - H tạo đầu ra có độ dài cố định
  - $H(x)$  tính toán mọi  $x$  tương đối dễ dàng, tạo điều kiện cho việc cài đặt trên phần cứng lẫn phần mềm được thiết thực
  - Với bất kỳ giá trị băm  $h$ , không thể tính được  $x$  sao cho  $H(x)=h$ . (H được gọi là hàm một chiều)
  - Tính bền xung đột yếu (weak collision resistance): với bất kỳ giá trị  $x$ , không thể tính được  $y \neq x$  sao cho  $H(y) = H(x)$ .
  - Tính bền xung đột mạnh (strong collision resistance): Không thể tính được một cặp  $(x, y)$  sao cho  $H(x) = H(y)$

203

- Một số giải thuật phổ biến: MD5, SHA-1, SHA-2, Whirpool, ... đều có cùng cấu trúc cơ bản là một hàm nén.
- Mỗi giải thuật băm sử dụng một hàm nén khác nhau
- Cấu trúc cơ bản của hàm băm gồm
  - $M$  là khối rõ
  - $IV$  là một vector khởi tạo
  - $F$  là một hàm nén
  - $+$  là một số dạng của toán tử cộng modular

204

- Cấu trúc cơ bản của hàm băm



205

- Công dụng cơ bản của hàm băm
  - Mã hóa thông điệp cộng với mã băm  
 $A \rightarrow B: E(K, [M \parallel H(M)])$ 
    - Bảo mật: chỉ A và B chia sẻ K
    - Chứng thực:  $H(M)$  được bảo vệ bằng mật mã
  - Mã hóa mã băm chia sẻ với khóa bí mật:  
 $A \rightarrow B: M \parallel E(K, H(M))$ 
    - Chứng thực:  $H(M)$  được bảo vệ bằng mật mã
  - Mã hóa khóa bí mật với mã băm của người gửi  
 $A \rightarrow B: M \parallel E(PR_A, H(M))$ 
    - Chứng thực và chữ ký số
      - $H(M)$  được bảo vệ bằng mật mã
      - Chỉ A có thể tạo  $E(PR_A, H(M))$

206



- Công dụng cơ bản của hàm băm (tt)
  - Mã hóa kết quả của © với khóa bí mật chia sẻ  
 $A \rightarrow B: E(K, [M \parallel E(PR_A, H(M))])$ 
    - Bảo mật: chỉ A và B chia sẻ K
    - Chứng thực và chữ ký số
  - Tính mã băm của thông điệp cộng với trị bí mật:  
 $A \rightarrow B: M \parallel H(M \parallel S)$ 
    - Chứng thực: Chỉ A và B chia sẻ S
  - Mã hóa kết quả của (e)  
 $A \rightarrow B: E(K, [M \parallel H(M \parallel S)])$ 
    - Chứng thực: chỉ A và B chia sẻ S
    - Bảo mật: chỉ A và B chia sẻ K

207

### 4.4.2 MD5 (Message Digest)

- Được phát minh bởi Ron Rivest tại đại học MIT
- Phát triển từ MD2, MD4
- Là thuật toán được sử dụng khá phổ biến
- Input: thông điệp với độ dài bất kỳ
- Output: giá trị băm (message digest) 128 bits
- Giải thuật gồm 5 bước thao tác trên khối 512 bits

208

### • Bước 1: đệm

- Bổ sung các bit đệm sao cho dữ liệu có độ dài  $l \equiv 448 \pmod{512}$  hay  $l = n * 512 + 448$  ( $n, l$  nguyên)
- Luôn thực hiện đệm dữ liệu ngay cả khi dữ liệu ban đầu có độ dài mong muốn. Ví dụ, dữ liệu có độ dài 448 được đệm thêm 512 bits để được độ dài 960 bits.
- Số lượng bit đệm thêm nằm trong khoảng 1 đến 512
- Các bit được đệm gồm 1 bit “1” và các bit 0 theo sau.



209

### • Bước 2: thêm vào độ dài

- Độ dài của khối dữ liệu ban đầu được biểu diễn dưới dạng nhị phân 64-bit và được thêm vào cuối chuỗi nhị phân kết quả của bước 1
- Nếu độ dài của khối dữ liệu ban đầu  $> 2^{64}$ , chỉ 64 bits thấp được sử dụng, nghĩa là giá trị được thêm vào bằng  $K \pmod{2^{64}}$
- Kết quả có được từ 2 bước đầu là một khối dữ liệu có độ dài là bội số của 512. Khối dữ liệu được biểu diễn:
  - Bằng một dãy  $L$  khối 512-bit  $Y_0, Y_1, \dots, Y_{L-1}$
  - Bằng một dãy  $N$  từ (word) 32-bit  $M_0, M_1, M_{N-1}$ .  
 $\rightarrow N = L \times 16$  ( $32 \times 16 = 512$ )



210

- Bước 3: khởi tạo bộ đệm MD (MD buffer)
  - Một bộ đệm 128-bit được dùng lưu trữ các giá trị băm trung gian và kết quả. Bộ đệm được biểu diễn bằng 4 thanh ghi 32-bit với các giá trị khởi tạo ở dạng little-endian (byte có trọng số nhỏ nhất trong từ nằm ở địa chỉ thấp nhất) như sau:
    - A = 67 45 23 01
    - B = EF CD AB 89
    - C = 98 BA DC FE
    - D = 10 32 54 76
  - Các giá trị này tương đương với các từ 32-bit sau:
    - A = 01 23 45 67
    - B = 89 AB CD EF
    - C = FE DC BA 98
    - D = 76 54 32 10

211

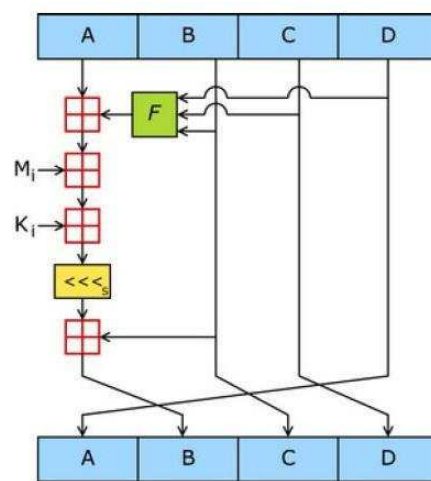
- Bước 4: xử lý các khối dữ liệu 512 bit
  - Hàm nén: gồm bốn vòng lặp xử lý có cấu trúc giống nhau nhưng sử dụng các hàm luận lý khác nhau gồm F, G, H, I
    - $F(X,Y,Z) = X \wedge Y \vee \neg X \wedge Z$
    - $G(X,Y,Z) = X \wedge Z \vee Y \wedge \neg Z$
    - $H(X,Y,Z) = X \text{ xor } Y \text{ xor } Z$
    - $I(X,Y,Z) = Y \text{ xor } (X \vee \neg Z)$
  - Mảng 64 phần tử được tính theo công thức  
 $T[i] = 2^{32} \times \text{abs}(\sin(i))$  (I được tính theo radian)
  - Kết quả của bốn vòng lặp được cộng (theo modulo  $2^{32}$  với đầu vào  $CV_q$  để tạo  $CV_{q+1}$
- Bước 5 - Xuất kết quả: Sau khi xử lý hết L khối 512-bit, đầu ra của lần xử lý thứ L là giá trị băm 128 bits.

212

- Tóm tắt giải thuật:
  - $CV_0 = IV$
  - $CV_{q+1} = \text{SUM}_{32}[CV_q, \text{RFI}(Y_q, \text{RFH}(Y_q, \text{RFG}(Y_q, \text{RFF}(Y_q, CV_q))))]$
  - $MD = CV_L - 1$
- Với các tham số
  - IV: bộ đệm gồm 4 thanh ghi ABCD
  - $Y_q$ : khối dữ liệu thứ  $q$  gồm 512 bits
  - L: số khối 512-bit sau khi đệm dữ liệu
  - $CV_q$ : đầu ra của khối thứ  $q$  sau khi áp dụng hàm nén
  - $\text{RFx}$ : hàm luận lý sử dụng trong các vòng (F,G,H,I)
  - MD: message digest – giá trị băm
  - $\text{SUM}_{32}$ : cộng modulo  $2^{32}$

213

- Hàm nén:
  - Mỗi vòng thực hiện 16 bước, mỗi bước thực hiện các phép toán để cập nhật giá trị buffer ABCD, mỗi bước được mô tả như sau
  - $A \leftarrow B + ((A + F(B,C,D) + X[k] + T[i]) \lll s)$
  - A,B,C,D: các từ của thanh ghi
  - F: một trong các hàm F,G,H,I
  - $\lll s$  : dịch vòng trái s bits
  - $M_i \sim X[k]$ : từ 32-bit thứ k của khối dữ liệu 512 bits.  $k=1..15$
  - $K_i \sim T[i]$ : giá trị thứ i trong bảng T.
  - +: phép toán cộng modulo  $2^{32}$



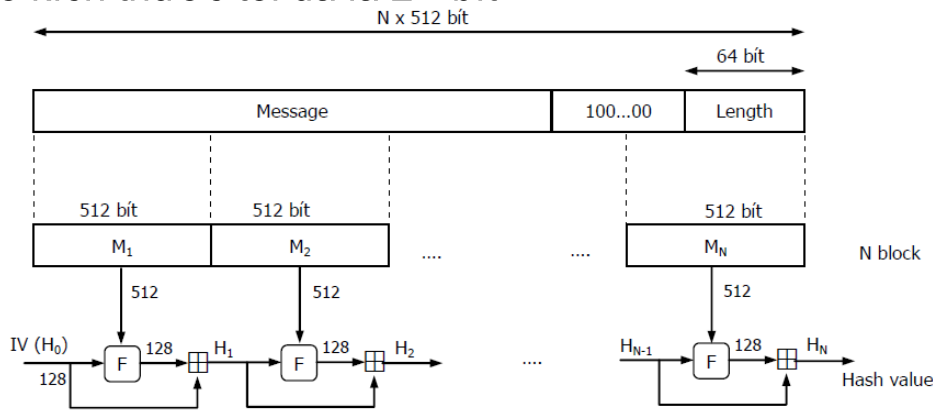
214

• Các giá trị trong bảng T:

T[1] = d76aa478	T[17] = f61e2562	T[33] = fffa3942	T[49] = f4292244
T[2] = e8c7b756	T[18] = c040b340	T[34] = 8771f681	T[50] = 432aff97
T[3] = 242070db	T[19] = 265e5a51	T[35] = 6d9d6122	T[51] = ab9423a7
T[4] = c1bdceee	T[20] = e9b6c7aa	T[36] = fde5380c	T[52] = fc93a039
T[5] = f57c0faf	T[21] = d62f105d	T[37] = a4beea44	T[53] = 655b59c3
T[6] = 4787c62a	T[22] = 2441453	T[38] = 4bdecfa9	T[54] = 8f0ccc92
T[7] = a8304613	T[23] = d8a1e681	T[39] = f6bb4b60	T[55] = ffeff47d
T[8] = fd469501	T[24] = e7d3fbc8	T[40] = bebfbc70	T[56] = 85845dd1
T[9] = 698098d8	T[25] = 21e1cde6	T[41] = 289b7ec6	T[57] = 6fa87e4f
T[10] = 8b44f7af	T[26] = c33707d6	T[42] = eaa127fa	T[58] = fe2ce6e0
T[11] = ffff5bb1	T[27] = f4d50d87	T[43] = d4ef3085	T[59] = a3014314
T[12] = 895cd7be	T[28] = 455a14ed	T[44] = 4881d05	T[60] = 4e0811a1
T[13] = 6b901122	T[29] = a9e3e905	T[45] = d9d4d039	T[61] = f7537e82
T[14] = fd987193	T[30] = fcfa3f8	T[46] = e6db99e5	T[62] = bd3af235
T[15] = a679438e	T[31] = 676f02d9	T[47] = 1fa27cf8	T[63] = 2ad7d2bb
T[16] = 49b40821	T[32] = 8d2a4c8a	T[48] = c4ac5665	T[64] = eb86d391

215

- Sơ đồ hàm băm MD5 với kích thước giá trị băm là 128 bit, được dùng để tính giá trị băm của thông điệp có kích thước tối đa là  $2^{64}$  bit



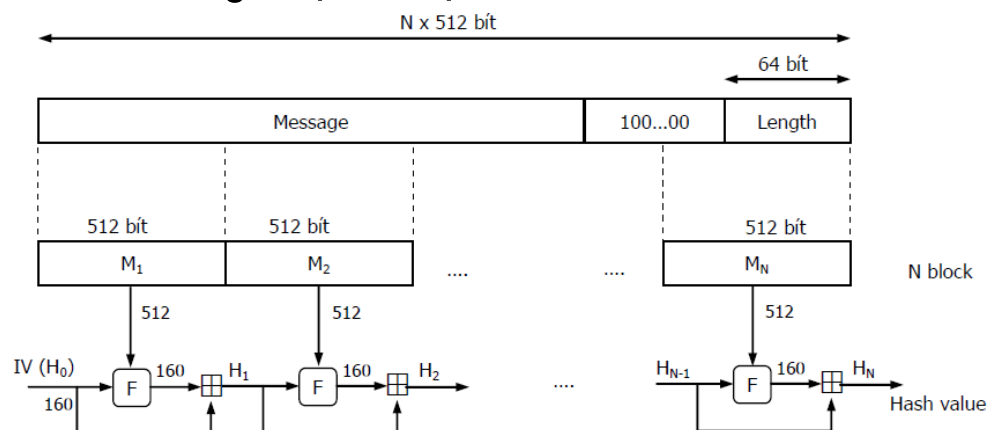
216

- Được phát triển bởi Viện Tiêu chuẩn và Công nghệ (NIST)
- Phiên bản 1995 được gọi là SHA-1, được định nghĩa trong RFC 3174
- Hàm băm SHA-1 với giá trị băm có kích thước là 160 bit, được dùng để tính giá trị băm của thông điệp có kích thước tối đa là  $2^{64}$  bit.

217

### SHA-1 (tt)

- Sơ đồ tổng thể của SHA1 tương tự MD5, nhưng kích thước của giá trị băm tại mỗi bước là 160 bit.



218

## 4.5 Chữ ký số (Digital signature)

- Là một định danh điện tử được tạo ra bởi máy tính được các tổ chức sử dụng nhằm đạt được tính hiệu quả và có hiệu lực như là các chữ ký tay.
- Là một cơ chế xác thực hóa cho phép người tạo ra thông điệp đính kèm một mã số vào thông điệp giống như là việc ký một chữ ký lên một văn bản bình thường.
- Chữ ký số (Digital signature) đảm bảo:
  - Authentication
  - Integrity
  - Non-repudiation

219

## 4.5 Chữ ký số (Digital signature)

- ☐ Đảm bảo tính xác thực
  - Chứng minh tính hợp pháp của người gửi
  - Chứng minh tính toàn vẹn của dữ liệu
- ☐ Chữ ký số là hàm của các tham số
  - Thông báo giao dịch (văn bản gốc)
  - Thông tin bí mật (Khóa riêng của người gửi)
- ☐ Thông tin công khai trên mạng (Khóa công khai)
- ☐ Mã xác thực : Đảm bảo toàn vẹn của thông điệp

220

- Nguyên lý: Alice muốn “ký” vào thông điệp  $m$  của mình, cô ta sẽ:
  - Mã hóa  $m$  bằng khóa bí mật của mình để nhận được bản mã  $\{m\}_{K\_private}$
  - Thông điệp  $\langle m, \{m\}_{K\_private} \rangle$  là thông điệp  $m$  được ký bởi Alice.
- Chữ ký điện tử  $\{m\}_{K\_private}$  chỉ có thể được tính toán bởi Alice vì cô ta sử dụng khóa bí mật của mình, vì vậy sẽ đảm bảo được:
  - Chứng thực (authentication): thông điệp này được Alice ký
  - Không từ chối trách nhiệm (Non-repudiation): Alice không thể chối bỏ việc ký này vì ngoài cô ta không ai có thể “ký” được “chữ ký” này.

221

- Kiểm tra chữ ký số
  - Khi nhận được thông điệp  $\langle m, \{m\}_{K\_private} \rangle$  được Alice ký
  - Ta giải mã chữ ký  $\{m\}_{K\_private}$  bằng khóa công khai của Alice để nhận được bản rõ  $m'$ .
  - So sánh  $m$  với  $m'$ . Nếu  $m \equiv m'$  th. thông điệp này chính là của Alice và nó không bị sửa đổi. Tính chất này đảm bảo tính toàn vẹn dữ liệu (integrity) của việc gửi-nhận dữ liệu.
- Tối ưu hóa chữ ký số:
  - Để tránh mã hóa toàn bộ thông điệp  $m$  bằng khóa bí mật (thường mất thời gian), ta chỉ mã hóa hàm băm của nó  $H(m)$  để nhận được  $\{H(m)\}_{K\_private}$ .

222



## Thuật mã RSA và Chữ ký số (tt)

### 1. Bên gửi

-Tạo bản MD của thông báo  $M \rightarrow H(M)$

-Dùng khóa riêng ( $d_s$ ) của người gửi mã hóa  $H(M)$ :

$$E(d_s, H(M))$$

-Truyền  $(M, E(d_s, H(M)), e_s)$  trong đó  $e_s$  là khóa công khai của người gửi

### 2. Bên nhận

-Tính MD của thông báo nhận được  $M' \rightarrow H(M')$

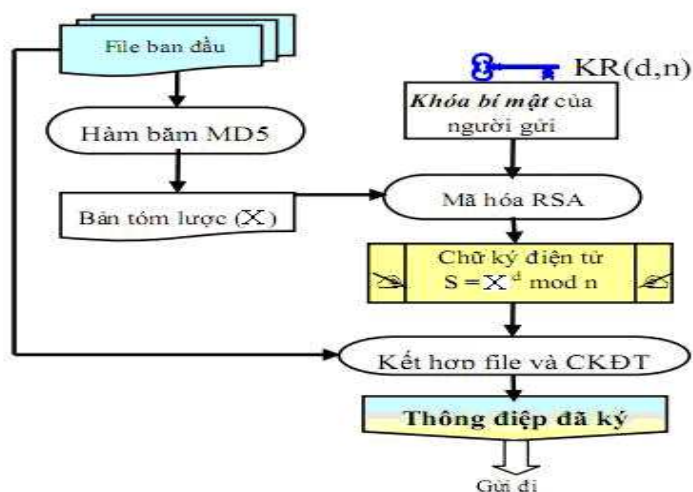
-Dùng khóa công khai của bên gửi ( $e_s$ ) giải mã thông điệp  $D(E(e_s H(M)))$  và so sánh kết quả với  $H(M')$

-Nếu kết quả trùng : xác thực đúng chữ ký của bên gửi .

Ngược lại không phải chữ ký bên gửi

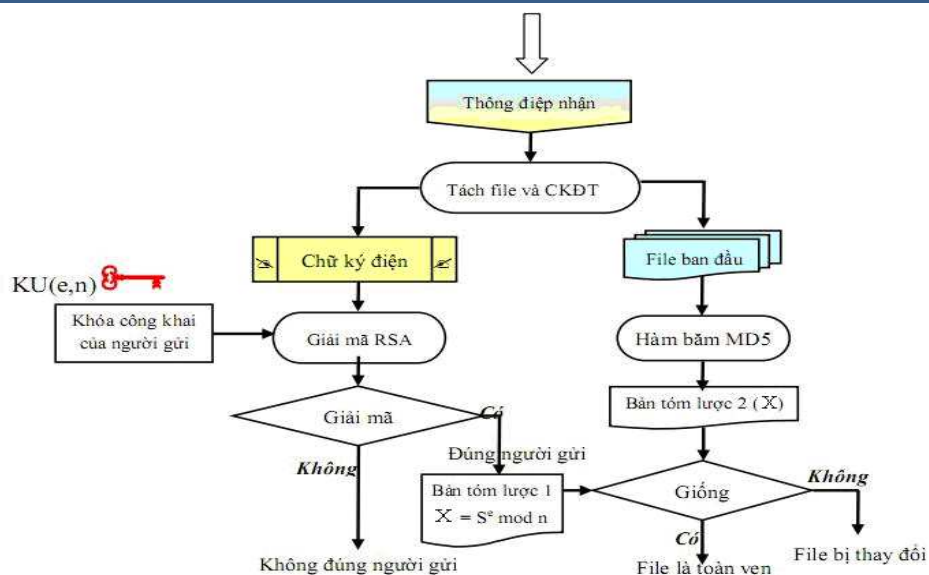
223

## Ký và gửi các file văn bản dùng SHA-1(MD5) & thuật toán RSA



224

## Kiểm tra Digital signature



225

## ÔN TẬP

### CÂU HỎI ÔN TẬP

226

- [1] Cryptography and Network Security: Principles and Practice – William Stallings (7th Edition) năm 2016
- [2] Modern Cryptography: Applied Mathematics for Encryption and Information Security - Chuck Easttom năm 2016
- [3] Mark Stamp, “Information security principles and practice”, JohnWiley & Sons, Inc., Hoboken, New Jersey, năm 2006.
- [4] Cryptography and Network Security Principles and Practices, 4th Edition William Stallings Prentice Hall 2005)
- [5] Introduction to Cryptography, Principles and Applications, Hans Delfs, Helmut Knebl, Springer năm 2007