

Chương 3

Hệ mã hóa cổ điển

Giáo viên: Lê Quốc Anh

Nội dung

1. Những khái niệm cơ bản về hệ mã hóa
2. Phân loại các hệ mã hóa
3. Hệ mã hóa cổ điển
 - ❑ Mã hóa Caesar
 - ❑ Mã hóa đơn bảng
 - ❑ Mã hóa Affine
 - ❑ Mã hóa Vigenère
 - ❑ Mã hóa Playfair
 - ❑ Mã hóa Hill
 - ❑ Mã hàng rào sắt

Slide 2

Giới thiệu

MẬT THƯ 1: 45, 24, 34 – 12, 11 – 13- 14, 35, 11, 34 – 31, 15, 45

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y



Slide 3

Giới thiệu

MẬT THƯ 2:

**TÍ VỀ - TUẤT THƯƠNG – HỢI NHẤT – SỬU
HƯỚNG – DẬU YÊU – DẦN MẬT – MỆO TRỜI – TỊ
SẾ - MÙI NGƯỜI – NGỌ THẤY – THÂN BẠN**



☞ **12 CON GIÁP: TÍ, SỬU, DẦN, MỆO,
THÌN, NGỌ, MÙI, THÂN, DẬU, TUẤT, HỢI**

Slide 4

Vấn Đề đặt ra: Tại sao chúng ta cần mã hóa?

- Mã hóa là một phương pháp hỗ trợ rất tốt trong việc chống lại những truy cập bất hợp pháp tới dữ liệu được truyền đi qua các kênh truyền thông.
- Mã hoá sẽ khiến cho nội dung thông tin được truyền đi dưới dạng mờ và không thể đọc được đối với bất kỳ ai cố tình muốn lấy thông tin đó.

Slide 5

1. Những khái niệm cơ bản về hệ mã hóa

- **Kỹ thuật mật mã (cryptology)** là ngành khoa học nghiên cứu 2 lĩnh vực: mã hóa (cryptography) và phân tích mật mã (cryptanalysis codebreaking)

Slide 6

1. Những khái niệm cơ bản về hệ mã hóa

- **Mã hóa (cryptography)** là ngành khoa học nghiên cứu các phương pháp và kỹ thuật đảm bảo an toàn và bảo mật dữ liệu trong việc truyền tin.
- Ứng dụng của mật mã:
 - Trong các cơ quan chính phủ: bảo vệ thông tin mật, các thông tin quân sự, ngoại giao, ...
 - Trong lĩnh vực kinh tế: bảo mật thông tin tài khoản ngân hàng, giao dịch thanh toán, thông tin khách hàng, ...
 - Trong y tế: bảo vệ thông tin cá nhân,
 - Trong bảo vệ thông tin cá nhân: thông tin riêng tư, tài khoản email, an toàn trên mạng xã hội, ...

Slide 7

1. Những khái niệm cơ bản về hệ mã hóa

- **Phân tích mật mã (cryptanalysis)**: ngành khoa học nghiên cứu các phương pháp, kỹ thuật nhằm phá vỡ hệ thống mã hóa.
- Trong sự phát triển của mật mã thì lĩnh vực mật mã và phân tích mật mã phát triển song hành với nhau, tuy nhiên trong học tập, nghiên cứu thì lĩnh vực mật mã học được quan tâm rộng rãi hơn do các ứng dụng thực tiễn, hiệu quả mà nó đem lại.

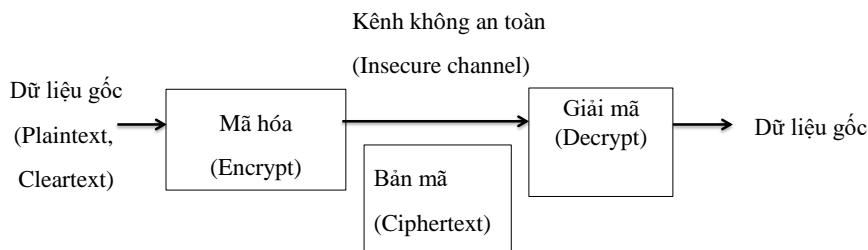
Slide 8

1. Những khái niệm cơ bản về hệ mã hóa

- **Giao thức mật mã (cryptographic protocol)** là tập hợp các quy tắc, trình tự thực hiện sơ đồ mã hóa.
- **Độ an toàn của hệ mã hóa:** là khả năng chống lại việc thám mã, trong nhiều trường hợp được tính bằng số phép toán cần thực hiện để thám mã sử dụng thuật toán tối ưu nhất.
- **Hệ thống mật mã (cryptosystem)** là hệ thống đảm bảo an toàn dữ liệu sử dụng công cụ mã hóa. Hệ thống mật mã bao gồm: sơ đồ, giao thức mật mã, quy tắc tạo và phân phối khóa. Khái niệm hệ thống mật mã có thể hiểu đơn giản hơn là bao gồm: thuật toán (algorithm) và giá trị mật (key).

Slide 9

Sơ đồ mã hóa



Mô hình toán học tổng quát:

Mã hóa: $C=E(P)$

Giải mã: $P=D(C)$,

với Plaintext (P), Encrypt (E), Ciphertext (C), Decrypt (D)

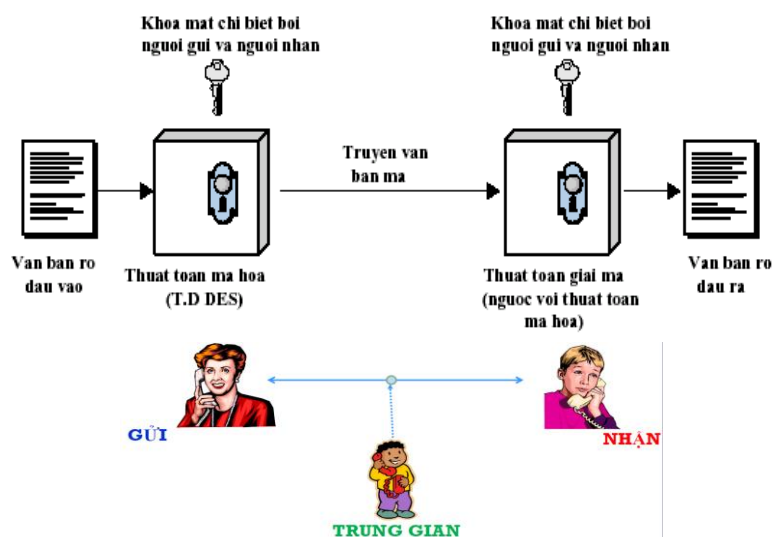
Slide 10

Những khái niệm cơ bản về hệ mã hóa

- **Văn bản gốc (plaintext)** là văn bản ban đầu có nội dung có thể đọc được và cần được bảo vệ.
- **Văn bản mã hóa (ciphertext)** là văn bản sau khi mã hóa, nội dung không thể đọc được.
- **Mã hóa (encryption)** là quá trình chuyển văn bản rõ thành văn bản mã hóa.
- **Giải mã (decryption)** là quá trình đưa văn bản mã hóa về lại văn bản gốc ban đầu

Slide 11

Mô hình đơn giản của Mật Mã



Slide 12

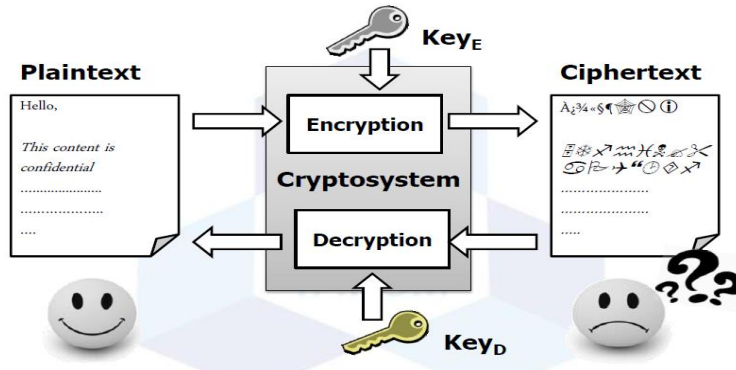
Hệ thống mã hóa



Hệ thống mã hóa (cryptosystem)

Cryptosystem = (encryption + decryption) algorithms

Khóa (key) được sử dụng trong quá trình mã hóa và giải mã



Slide 13

Vai trò của hệ mật mã

- Hệ mật mã phải che dấu được nội dung của văn bản rõ (PlainText).
- 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).
- Tổ chức các sơ đồ chữ ký điện tử, đảm bảo không có hiện tượng giả mạo, mạo danh để gửi thông tin trên mạng.

Slide 14

Các thành phần của một hệ mật mã

Một hệ mật mã là bộ 5 (P, C, K, E, D) thoả mãn các điều kiện sau:

- P là không gian bản rõ: là tập hữu hạn các bản rõ có thể có.
- C là không gian bản mã: là tập hữu hạn các bản mã có thể có.
- K là không gian khoá: là tập hữu hạn các khoá có thể có.

Đối với mỗi $k \in K$ có một quy tắc mã $e_k: P \rightarrow C$ và một quy tắc giải mã tương ứng $d_k \in D$.

Với mỗi $e_k: P \rightarrow C$ và $d_k: C \rightarrow P$ là những hàm mà $d_k(e_k(x))=x$ với mọi bản rõ $x \in P$.

Hàm giải mã d_k chính là ánh xạ ngược của hàm mã hóa e_k

Slide 15

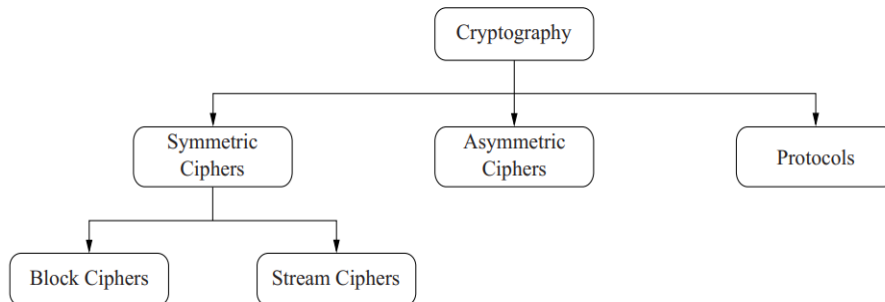
2. Phân loại các hệ mã hóa

- Theo thời gian có thể chia mật mã thành
 - Mã hóa cổ điển (classical cryptographic)
 - Mã hóa hiện đại (modern cryptography)
- **Mã hóa cổ điển (classical cryptographic):** đây là kỹ thuật được hình thành từ xa xưa, dựa trên hai kỹ thuật cơ bản: thay thế (substitution) và hoán vị (transposition).
- Do đó, độ an toàn của kỹ thuật này không cao do chỉ dựa vào sự che giấu thuật toán, hiện nay mã hóa cổ điển ít được sử dụng trong thực tế.

Slide 16

2. Phân loại các hệ mã hóa

- **Mã hóa hiện đại (modern cryptography):** mã hóa đối xứng (symmetric cipher, secret key cryptography – 1 khóa), bất đối xứng (asymmetric cipher, public key cryptography – 2 khóa), hàm băm (hash functions – không có khóa).



Slide 17

3. Mã hóa cổ điển (classical cryptographic)

- **Mã hóa cổ điển** dựa trên kỹ thuật thay thế (thay thế kí tự hoặc các kí tự này bằng kí tự hoặc các kí tự khác tương ứng) và hoán vị (thay đổi trật tự, vị trí các ký tự) trong văn bản gốc. Các kỹ thuật này có thể áp dụng đối với một ký tự (monoalphabetic) hoặc nhiều ký tự (polyalphabetic) tùy vào mục đích sử dụng.
- Một số hệ mã cổ điển
 - Mã hóa Caesar
 - Mã hóa đơn bảng
 - Mã hóa Affine
 - Mã hóa Vigenère
 - Mã hóa Playfair
 - Mã hóa Hill
 - Mã hàng rào sắt

Hệ mã cổ điển sử dụng kỹ thuật thay thế

Hệ mã cổ điển sử dụng kỹ thuật hoán vị

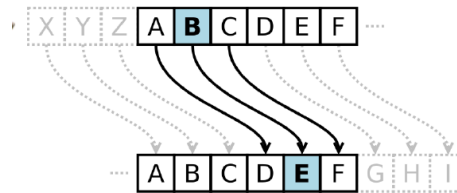
Slide 18

Mã hóa Caesar

- Thế kỷ thứ 3 trước công nguyên, Julius Ceasar đưa ra phương pháp mã hóa này.
- **Thay thế mỗi ký tự trong bản rõ bằng ký tự đứng sau nó k vị trí trong bảng chữ cái.**
- Giả sử chọn $k=3$, ta có bảng chuyển đổi:

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



Slide 19

Mã hóa Caesar

- 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:



Slide 20

Mã hóa Caesar

- Hệ mã Caesar là một hệ mã hoá thay thế đơn âm làm việc trên bảng chữ cái tiếng Anh 26 ký tự (A, B, ..., Z).
- Không gian bản rõ P là các thông điệp được tạo từ bảng mã A, Không gian bản mã $C \equiv P$, giả sử số phần tử của bảng mã $|A| = N$. Với hệ mã Caesar sử dụng bảng chữ cái tiếng anh 26 ký tự nên $N=26$
- Để mã hóa người ta đánh số các chữ cái từ 0 tới N-1.
- Không gian khóa $K = Z_N$. Với mỗi khóa $k \in K$ hàm mã hóa và giải mã một ký tự có số thứ tự là i sẽ được thực hiện như sau:
- Công thức mã hóa: $E_K(i) = (i + k) \bmod N$
- Công thức giải mã: $D_K(i) = (i - k) \bmod N$

Slide 21

Mã hóa Caesar

- Hệ mã Caesar sử dụng bảng mã là bảng chữ cái tiếng anh 26 ký tự.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Công thức mã hóa: $E_K(i) = (i + k) \bmod 26$
- Công thức giải mã: $D_K(i) = (i - k) \bmod 26$
- Với $k=3$ được Caesar sử dụng làm khóa
- Ví dụ:
 - Mã hóa xâu P = "DAI HOC VINH" với $k = 3$
 - Giải mã xâu C = " ABC UIK" với $k = 3$

Slide 22

Mã hóa Caesar

- Để tấn công hệ mật Caesar có thể sử dụng một số kỹ thuật sau:
- Vét cạn (brute-force): thử tất cả các khả năng biến đổi có thể xảy ra để tìm được quy tắc thay thế, do hệ mã Caesar chỉ có 26 ký tự (tương ứng 25 quy tắc - khóa) nên việc giải mã không mất nhiều thời gian trong điều kiện hiện nay.
- Tần số xuất hiện kí tự (Character frequencies): dựa vào thống kê xuất hiện của các kí tự trong bản mã, đối chiếu với bảng tần số được khảo sát trước của từng ngôn ngữ.

Slide 23

Mã hóa Caesar

- Trong 25 trường hợp trên, chỉ có trường hợp $k=3$ thì bản giải mã tương ứng là có ý nghĩa.
- Do đó có thể chắc chắn rằng **“meet me after the toga party”** là bản rõ ban đầu.

KEY	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1	oggv	og	chvgt	vjg	vqic	rctva
2	nffu	nf	bgufs	uif	uphb	qbsuz
3	meet me after the toga party					
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	objv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlg
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puitg	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrng	zr	nsgre	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzlx	znk	zumg	vgxze
24	rjyy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

Slide 24

Mã hóa Caesar

Bài tập:

1. Áp dụng mã Ceasar mã hóa bản rõ sau với khóa $k = 4$
actions speak louder than words

2. Đoán khóa k và giải mã cho bản mã sau:
ST RFS HFS XJWAJ YBT RFXIJWX

Slide 25

Mã hóa đơn bảng

- Phương pháp đơn bảng tổng quát hóa phương pháp Ceasar bằng cách dòng mã hóa không phải là một dịch chuyển k vị trí của các chữ cái A, B, C, ... nữa mà là một *hoán vị* của 26 chữ cái này. Lúc này mỗi hoán vị được xem như là một khóa.
- Việc mã hóa được tiến hành bằng cách thay thế một chữ cái trong bản rõ thành một chữ cái trong bản mã, nên phương pháp này được gọi là phương pháp thay thế.

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

Plaintext: ifwewishtoreplaceletters

Ciphertext: WIRFRWAJUH YFTSDVFSFUUFYA

Slide 26

Mã hóa đơn bảng

- Số lượng hoán vị của 26 chữ cái là $26! = 4 \times 10^{26}$ (tương đương với số khóa).
- Vì $26!$ là một con số khá lớn \rightarrow tấn công phá mã vét cạn khóa là bất khả thi (6400 thiên niên kỷ với tốc độ thử khóa là 109 khóa/giây).

\rightarrow phương pháp này được xem là một phương pháp mã hóa an toàn trong suốt 1000 năm sau công nguyên.

- 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:



Slide 27

Mã hóa đơn bảng

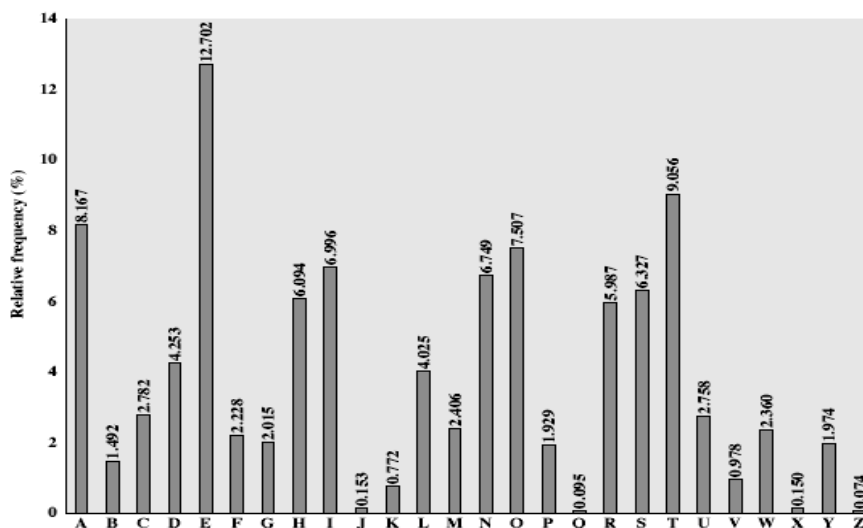
- Tuy nhiên vào thế kỷ thứ 9, một nhà hiền triết người Ả Rập tên là Al-Kindi đã phát hiện ra một phương pháp phá mã khả thi khác. Phương pháp phá mã này dựa trên nhận xét sau:
 - Trong ngôn ngữ tiếng Anh, tần suất sử dụng của các chữ cái không đều nhau, chữ E được sử dụng nhiều nhất, còn các chữ ít được sử dụng thường là Z, Q, J. Tương tự như vậy, đối với cụm 2 chữ cái (digram), cụm chữ TH được sử dụng nhiều nhất.
 - Nếu chữ E được thay bằng chữ K thì tần suất xuất hiện của chữ K trong bản mã là 13.05%. Đây chính là cơ sở để thực hiện phá mã.

Slide 28

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

Bảng 2-2. Bảng liệt kê tần suất chữ cái tiếng Anh

Mã hóa đơn giản



Slide 30

Mã hóa đơn bảng

- Cho bản mã:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPPDPTGUDTMOHMQ

- Đếm tần suất ký tự

A 2	F 3	K 0	P 17	U 9
B 2	G 3	L 0	Q 3	V 5
C 0	H 6	M 7	R 0	W 4
D 6	I 1	N 0	S 10	X 5
E 6	J 0	O 9	T 4	Y 2

DT 2	HZ 2	PE 2	TS 2	XU 2
DZ 2	MO 2	PO 3	UD 2	ZO 2
EP 3	OH 2	PP 2	UZ 3	ZS 2
FP 3	OP 3	SX 3	VU 2	ZU 2
HM 2	PD 3	SZ 2	WS 2	ZW 3

Số lần xuất hiện của các digram
(xuất hiện từ 2 lần trở lên) là:

Slide 31

Mã hóa đơn bảng

- Do đó ta có thể đoán P là mã hóa của e, Z là mã hóa của t. Vì TH có tần suất cao nhất trong các digram nên trong 4 digram ZO, ZS, ZU, ZW có thể đoán ZW là th.
- Chú ý rằng trong dòng thứ nhất có cụm ZWSZ, nếu giả thiết rằng 4 chữ trên thuộc một từ thì từ đó có dạng th_t, từ đó có thể kết luận rằng S là mã hóa của a (vì từ THAT có tần suất xuất hiện cao).
- Như vậy đến bước này, ta đã phá mã được như sau:

Slide 32

Mã hóa đơn giản

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a e e te a that e e a a
 VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
 e t ta t ha e ee a e th t a
 EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e e e tat e the t

it was disclosed yesterday that several informal but
 direct contacts have been made with political
 representatives of the viet cong in moscow

Slide 33

Mã hóa Affine

- Không gian bản rõ và bản mã $P \equiv C \equiv Z_n$
- Không gian khóa $K = \{(a, b) \in Z_n \times Z_n: \text{GCD}(a, n) = 1\}$
- Với mỗi khóa $k = (a, b) \in K$, định nghĩa
- Hàm mã hóa: $e_k(x) = (ax + b) \bmod n$
- Hàm giải mã: $d_k(x) = a^{-1}(y - b) \bmod n$
- Với $x, y \in Z_n$
- $E = \{e_k, k \in K\}$ và $D = \{d_k, k \in K\}$
- **Lưu ý:** a và n phải nguyên tố cùng nhau $\text{GCD}(a, n) = 1$

Slide 34

Mã hóa Affine

- Giả sử xét bảng mã là bảng chữ cái tiếng anh 26 ký tự.
- $P \equiv C \equiv Z_{26}$
- Hàm mã hóa: $e_k(x) = (ax + b) \bmod 26$
- Hàm giải mã: $d_k(x) = a^{-1}(y - b) \bmod 26$
- a và 26 phải nguyên tố cùng nhau. $\text{GCD}(a, 26) = 1$
- $a \in Z_{26}$. Trong vành đồng dư Z_{26} có bao nhiêu chữ số nguyên tố cùng nhau với 26 ?

Slide 35

Bài tập: Mã hóa Affine

Bài 1:

$a = 5, b = 3: y = 5x + 3 \pmod{26}$.

Mã hoá: P = ANTOANTHONGTIN

Bài tập 3.9: Giả sử hệ mã Affine được cài đặt trên Z_{126} .

- a) Hãy xác định số khóa có thể có của hệ mã.
- b) Giả sử khóa mã hóa là (23, 7), hãy xác định khóa giải mã.

Slide 36

Bài tập: Mã hóa Affine

Bài tập 3.5: Cho hệ mã Affine được cài đặt trên Z_{99} . Khi đó khóa là các cặp (a, b) trong đó $a, b \in Z_{99}$ với $(a, 99) = 1$. Hàm mã hóa $E_K(x) = (a * x + b) \bmod 99$ và hàm giải mã $D_K(x) = a^{-1} * (x - b) \bmod 99$.

- Hãy xác định số khóa có thể được sử dụng cho hệ mã này.
- Nếu như khóa giải mã là $K^{-1} = (16, 7)$, hãy thực hiện mã hóa xâu $m = \text{"DANGER"}$.

Slide 37

Mã hóa Vigenère

- Thế kỷ thứ 15, một nhà ngoại giao người Pháp tên là **Vigenere** đã tìm ra phương án mã hóa thay thế đa bảng.
- Mã hóa Vigenere được hình thành trên mã hóa Caesar có sử dụng khóa (chuỗi các chữ cái) trên văn bản gốc (gồm các chữ cái).
- Mã hóa Vigenere là sự kết hợp của nhiều phép mã hóa Caesar với các bước dịch chuyển khác nhau.
- Để mã hóa, sử dụng bảng mã Vigenere (*Hình x*) với cột dọc là chuỗi khóa (khóa được lặp đi lặp lại để chiều dài tương ứng với văn bản gốc), cột ngang – văn bản gốc, giao giữa kí tự tương ứng cột chứa khóa và văn bản gốc chính là kí tự mã của thuật toán.

Slide 38

Mã hóa Vigenère

		PLAINTEXT LETTER																									
KEYWORD LETTER	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	

Slide 39

Mã hóa Vigenère

- Phương pháp Vigenere sử dụng khóa có độ dài m .
- Không gian khóa K của phương pháp Vigenere có số phần tử là n^m
- Ví dụ: $n=26$, $m=5$ thì không gian khóa $\sim 1.1 \times 10^7$

Chọn số nguyên dương m . Định nghĩa $P = C = K = (\mathbb{Z}_n)^m$

$$K = \{(k_1, k_2, \dots, k_m) \in (\mathbb{Z}_n)^m\}$$

Với mỗi khóa $k = (k_1, k_2, \dots, k_m) \in K$, định nghĩa:

$$e_k(x_1, x_2, \dots, x_m) = ((x_1 + k_1) \bmod n, (x_2 + k_2) \bmod n, \dots, (x_m + k_m) \bmod n)$$

$$d_k(y_1, y_2, \dots, y_m) = ((y_1 - k_1) \bmod n, (y_2 - k_2) \bmod n, \dots, (y_m - k_m) \bmod n)$$

với $x, y \in (\mathbb{Z}_n)^m$.

Slide 40

Mã hóa Vigenère

Ví dụ: $m = 6$ và keyword là **CIPHER**

Suy ra, khóa $k = (2, 8, 15, 7, 4, 17)$

Cho bản rõ: **thiscryptosystemisnotsecure**

19	7	8	18	2	17	24	15	19	14	18	24
2	8	15	7	4	17	2	8	15	7	4	17
21	15	23	25	6	8	0	23	8	21	22	15

18	19	4	12	8	18	13	14	19	18	4	2
2	8	15	7	4	17	2	8	15	7	4	17
20	1	19	19	12	9	15	22	8	25	8	19

20	17	4
2	8	15
22	25	19

Vậy bản mã là: **“vpxzgiaxivwoubttmjpwizitwzt”**

Slide 41

Mã hóa Vigenère

Bài tập:

Bài tập 3.14: Cho hệ mã Vigenere có $M = 6$. Mã hóa xâu $P = \text{“THIS IS MY TEST”}$ người ta thu được bản mã là **“LLKJML ECVVWM”**.

- Hãy tìm khóa mã hóa đã dùng của hệ mã trên.
- Dùng khóa tìm được ở phần trên hãy giải mã bản mã $C = \text{“KLGZWT OMBRVW”}$.

Slide 42

Mã hóa Playfair

- Được biết như là **mã thay thế đa ký tự**
- Được đề xuất bởi Charles Wheatstone, được mang tên của người bạn Baron Playfair
- ***Mã hóa Playfair 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.***

Slide 43

Mã hóa Playfair

- Mật mã đa ký tự (mỗi lần mã 2 ký tự liên tiếp nhau)
- Giải thuật dựa trên một ma trận các chữ cái 5×5 được xây dựng từ một khóa (chuỗi các ký tự)
- 1. Xây dựng ma trận khóa
 - Lần lượt thêm từng ký tự của khóa vào ma trận
 - Nếu ma trận chưa đầy, thêm các ký tự còn lại trong
 - bảng chữ cái vào ma trận theo thứ tự A - Z
 - I và J là xem như 1 ký tự
 - Các ký tự trong ma trận không được trùng nhau
- 2. Mã hóa
- 3. Giải mã

Slide 44

Mã hóa Playfair

- Dựa trên ma trận 5 × 5 của các ký tự được xây dựng bằng từ khóa (keyword)

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

- Trong ma trận trên, khóa là từ MONARCHY được điền vào các dòng đầu của bảng, các chữ cái còn lại của bảng chữ cái được điền tiếp theo một cách tuần tự. Riêng hai chữ I, J được điền vào cùng một ô

Slide 45

Mã hóa Playfair

- Bản rõ được mã hóa một lần 2 ký tự theo quy tắc sau:
 - Cặp hai ký tự giống nhau xuất hiện trong bản rõ sẽ được tách ra bởi 1 ký tự lọc, chẳng hạn như **x**. Ví dụ trước khi mã hóa “**balloon**” sẽ được biến đổi thành “**ba**x**lloxon**”.
 - Hai ký tự trong cặp đều rơi vào cùng một hàng, thì mã mỗi ký tự bằng ký tự bên phải nó trong cùng hàng của ma trận khóa, nếu nó là phần tử cuối của hàng thì vòng sang ký tự đầu cùng của hàng, chẳng hạn “**ar**” mã hóa thành “**rm**”

Slide 46

Mã hóa Playfair

3. Hai ký tự mà rơi vào cùng một cột thì nó được mã bằng ký tự ngay dưới, nếu nó ở cuối cột thì vòng sang ký tự ở đầu cột, chẳng hạn “**mu**” được mã hóa thành “**CM**”, ov được mã hóa thành HO
4. Trong trường hợp khác, mỗi ký tự của bản rõ trong một cặp được thay bởi ký tự nằm cùng hàng với nó và cột là cùng cột với ký tự cùng cặp. Chẳng hạn, “**hs**” mã thành “**bp**”, và “**ea**” mã thành “**im**” hoặc “**jm**”

Slide 47

Mã hóa Playfair

Phá mã

- An toàn được cải tiến hơn với mã hóa đơn bản (simple monoalphabetic ciphers)
- Chỉ xét trên 26 ký tự thì mã khóa Playfair có $26 \times 26 = 676$ cặp ký tự.
→ các cặp ký tự này ít bị chênh lệch về tần suất hơn so với sự chênh lệch tần suất của từng ký tự. Ngoài ra số lượng các cặp ký tự nhiều hơn cũng làm cho việc phá mã tần suất khó khăn hơn. Đây chính là lý do mà người ta tin rằng mã hóa Playfair không thể bị phá và được quân đội Anh sử dụng trong chiến tranh thế giới lần thứ nhất.
- Tuy nhiên, nó có thể bị bẻ khóa nếu cho trước vài trăm chữ, vì bản mã vẫn còn chứa nhiều cấu trúc của bản rõ.

Slide 48

Mã hóa Playfair

Ví dụ: Hãy tìm hiểu quá trình mã hóa và giải mã bằng phương pháp mã Playfair

Bản rõ: NGANHCNTTDHV

Khóa: smythework



Slide 49

Mã hóa Playfair

Bài tập:

Hãy tìm hiểu quá trình mã hóa và giải mã bằng phương pháp mã Playfair

Bản rõ P= “Đại học Vinh”

Khóa K=tinhoc

Slide 50

Hệ mã Hill

- 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:

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

Slide 51

Hệ mã 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 .

Slide 52

Hệ mã 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 xâu $P = \text{"HELP"}$ và giải mã ngược lại bản mã thu được.

Slide 53

Hệ mã Hill

Để mã hóa chúng ta chia xâu bản rõ thành hai vectơ 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 $C = \text{"DPLE"}$.

Slide 54

Hệ mã Hill

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 $\det(K) = (k_{11} * k_{22} - k_{21} * k_{12}) \bmod N$ là một phần tử có phần tử

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

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

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 Ơclit mở rộng tìm được $\det(K)^{-1} = 3$. Vậy $K^{-1} = 3 *$

$$\begin{pmatrix} 5 & 23 \\ 24 & 3 \end{pmatrix} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}.$$

Slide 55

Hệ mã Hill

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

Tương tự giải mã xâu $C = \text{"LE"}$ kết quả sẽ được 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.

Slide 56

Hệ mã Hill

Bài tập 3.12: Cho hệ mã Hill có $M = 2$.

- a) Ma trận $A = \begin{bmatrix} 15 & 13 \\ 7 & a \end{bmatrix}$ được sử dụng làm khóa cho hệ mã trên. Hãy tìm tất cả các khóa có thể sử dụng của hệ mã trên.
- b) Giả sử người ta sử dụng hệ mã trên để mã hóa bản rõ $P = \text{"MARS"}$ và thu được bản mã là "YARH" . Hãy thực hiện giải mã với bản mã là $C = \text{"MANNTF"}$ và đưa ra bản rõ.

Slide 57

Hệ mã Hill

Bài tập 3.11: Cho hệ mã Hill có $M = 2$.

- a) Ma trận $A = \begin{bmatrix} 5 & 3 \\ 11 & a \end{bmatrix}$ được sử dụng làm khóa cho hệ mã trên. Hãy tìm tất cả các khóa có thể sử dụng của hệ mã trên.
- b) Giả sử người ta sử dụng hệ mã trên để mã hóa bản rõ $P = \text{"EASY"}$ và thu được bản mã là "UMQA" . Hãy thực hiện giải mã với bản mã là $C = \text{"MCDZUZ"}$ và đưa ra bản rõ.

Slide 58

Mã hàng rào sắt (rail fence cipher)

- Đây là một mã dùng phép hoán vị hoặc chuyển vị, vì vậy gọi là mã hoán vị hoặc mã chuyển vị (***classical transposition or permutation ciphers***)
- Thực hiện xáo trộn thứ tự các ký tự trong bản rõ. Do thứ tự của các ký tự bị mất đi nên người đọc không thể hiểu được ý nghĩa của bản tin dù các chữ đó không thay đổi.
- Đơn giản nhất của mã hóa kiểu này là mã **rail fence cipher**

Slide 59

Mã hàng rào sắt (rail fence cipher)

- Ghi các ký tự trong bản rõ theo từng hàng rào, sau đó kết xuất bản mã dựa trên cột. Sau đó đọc bản mã theo từng hàng
- Ví dụ: bản rõ “meet me after the toga party” với hàng rào sắt độ sâu là 2 (Tách bản rõ thành 2 hàng)
- Ví dụ: bản rõ “meet me at the toga party” được viết thành

```
m e m a t e o a a t
e t e t h t g p r y
```

Cho bản mã

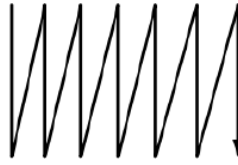
```
MEMATEOAATETETHTGPRY
```

Slide 60

Mã hàng rào sắt (rail fence cipher)

- Ví dụ bản rõ “attackpostponeduntilthisnoon” được viết lại thành bảng 4 x 7 như sau:

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



- Khi kết xuất theo từng cột thì có được bản mã:
“AODHTSUITTNSAPTNCIOIKNLOPETN”

Slide 61

Mã hàng rào sắt (rail fence cipher)

- Để an toàn hơn nữa, có thể áp dụng phương pháp hoán vị 2 lần (**double transposition**), tức sau khi hoán vị lần 1, ta lại lấy kết quả đó hoán vị thêm một lần nữa.
- Để phá mã phương pháp hoán vị 2 lần không phải là chuyện dễ dàng vì rất khó đoán ra được quy luật hoán vị.
- Ngoài ra không thể áp dụng được phương pháp phân tích tần suất chữ cái giống như phương pháp thay thế vì tần suất chữ cái của bản rõ và bản mã là giống nhau.

Slide 62

Mã hàng rào sắt (rail fence cipher)

- Một cơ chế phức tạp hơn là chúng ta có thể hoán vị các cột trước khi kết xuất bản mã.
- Ví dụ chọn một khóa là **MONARCH**, ta có thể hoán vị các cột:

Bản rõ “attackpostponeduntilthisnoon”

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

và có được bản mã: “APT NKNLOPETNAODHTT NSTSUI COIO”.

Việc giải mã được tiến hành theo thứ tự ngược lại.

Slide 63

Mã hàng rào sắt (rail fence cipher)

- Để an toàn hơn nữa => **hoán vị 2 lần** (double transposition):
- Sau khi hoán vị lần 1, ta lấy kết quả đó hoán vị lần nữa:

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
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

- Và cuối cùng **bản mã** là:
“NTTCNASILOTOAODSTETIPPHUKNNO”
- **Phá mã** phương pháp hoán vị 2 lần không phải là chuyện dễ dàng vì rất khó đoán ra được quy luật hoán vị.
- Không thể áp dụng được phương pháp phân tích tần suất chữ cái giống như phương pháp thay thế vì tần suất chữ cái của bản rõ và bản mã là giống nhau.

Slide 64

Mã hàng rào sắt (rail fence cipher)

Bài tập:

1. Bản rõ “attack at midnight” với hàng rào sắt độ sâu là 2

2. Mã hóa thông điệp sau bằng phương pháp hoán vị:

Bản rõ: **we are all together**

Khóa: **24153**

Slide 65

Xin chân thành cảm ơn!

Slide 66