Bài 2
Mã cổ điển

Thời lượng: 3 tiết

Lương Thái Lê

Nội dung

1. Tổng quan về mã cổ điển
2. Mã đối xứng và các khái niệm cơ bản
3. Các đặc trưng của một hệ mật mã
4. Mã thế
5. Mã hoán vị
6. Mã tích

1.1. Tổng quan về mã cổ điển

- Là phương pháp mã hóa đơn giản nhất
- Là cơ sở để phát triển các thuật toán mã hóa đối xứng ngày nay
  - Mọi mã cổ điển là mã đối xứng
- 2 loại mã cổ điển
  - Mã thay thế (Mã thế)
  - Mã hoán vị (Mã chuyển vị)

1.2. Tổng quan về mã cổ điển (tiếp)

- ***Mã 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.
  - Một số loại mã thay thế điển hình: Mã Ceasar, mã Playfair…

1.3. Tổng quan về mã cổ điển (tiếp)

- ***Mã chuyển vị:***
  - Là phương pháp mà các kí tự trong bản rõ vẫn được giữ nguyên, chúng chỉ được sắp xếp lại vị trí để tạo ra bản mã. Tức là các kí tự trong bản rõ hoàn toàn không bị thay đổi bằng kí tự khác mà chỉ đảo chỗ của chúng để tạo thành bản mã.
  - Một số loại mã chuyển vị điển hình: Rain Fence, dịch chuyển dòng…

Nội dung

1. Tổng quan về mã cổ điển
2. Mã đối xứng và các khái niệm cơ bản
3. Các đặc trưng của một hệ mật mã
4. Mã thế
5. Mã hoán vị
6. Mã tích

2.1. Mã đối xứng

- Sử dụng cùng 1 khóa **K** cho việc mã hóa và giải mã
  - là mã một khoá: khoá mã hoá = khoá giải mã
  - mã khoá chia sẻ
- Người gửi và người nhận chia sẻ khoá chung
- Mọi thuật toán mã cổ điển đều là mã đối xứng
- Là kiểu duy nhất trước khi phát minh ra khoá mã công khai vào những năm 1970
- Đến nay vẫn được sử dụng rộng

2.2. Các khái niệm cơ bản

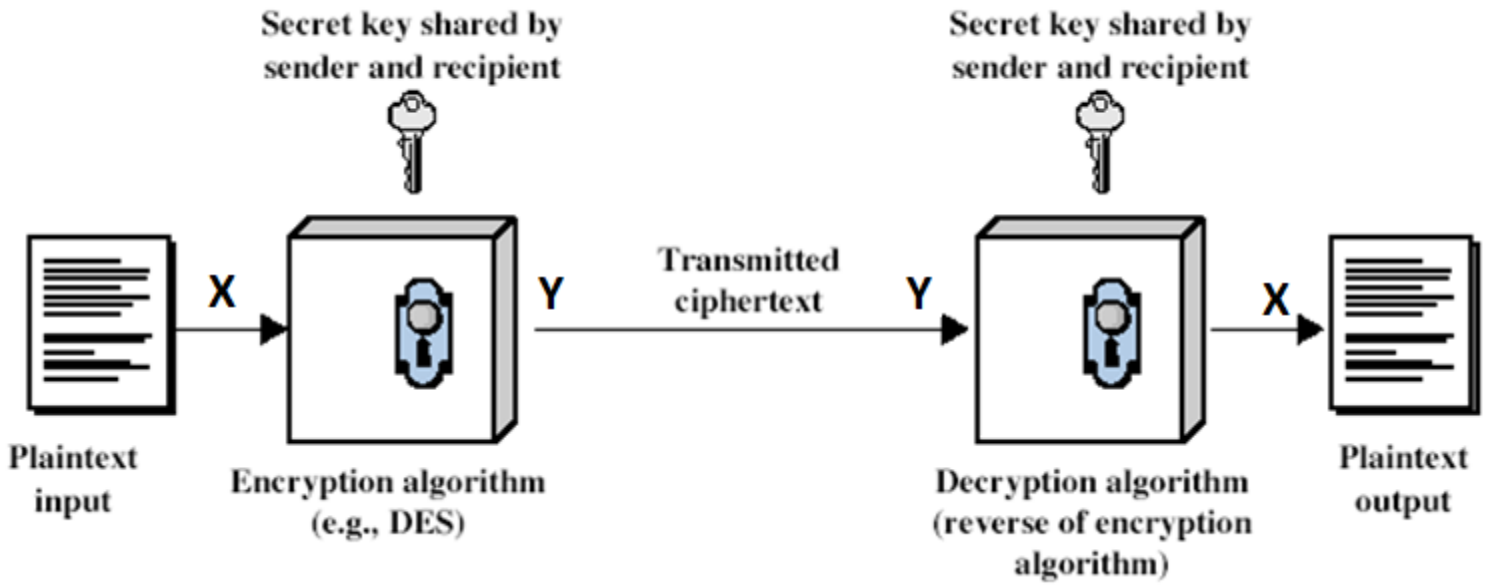
- **Bản rõ (X)** là bản tin gốc.
  - Có thể được chia nhỏ
- **Bản mã (Y)** là bản tin gốc đã được mã hoá.
  - thường có kích thước giống bản gốc
- **Mã** là thuật toán chuyển bản rõ thành bản mã
- **Khoá (K)** là thông tin (tham số) dùng để mã hoá
  - chỉ có người gửi và người nhận biết.
  - độc lập với bản rõ

2.2. Các khái niệm cơ bản (tiếp)

- **Mã hoá (E):**quá trìnhchuyển bản rõ thành bản mã
- **Giải mã (D):** quá trình chuyển bản mã thành bản rõ.
- **Mật mã:** nghiên cứu các nguyên lý và phương pháp mã hoá.
- **Thám mã:** nghiên cứu các nguyên lý và phương pháp giải mã mà không biết khoá.
- **Lý thuyết mã** bao gồm cả mật mã và thám mã

  =>để đánh giá độ mạnh của mã

2.3. Mô hình mã đối xứng
Symmetric Cipher Model



Về mặt toán học:

$$Y = E_K(X)$$
$$X = D_K(Y)$$

2.4. Các yêu cầu của mã đối xứng

- Hai yêu cầu để sử dụng an toàn mã khoá đối xứng là:

1. thuật toán mã hoá mạnh

   => có thể công khai thuật toán nhưng khó thám mã

2. khoá mật chỉ có người gửi và người nhận biết

   $\Rightarrow$có kênh an toàn để phân phối khóa.

   $\Rightarrow$khó tìm được mối liên hệ giữa khóa với bản mã

Nội dung

1. Tổng quan về mã cổ điển
2. Mã đối xứng và các khái niệm cơ bản
3. Các đặc trưng của một hệ mật mã
4. Mã thế
5. Mã hoán vị
6. Mã tích

3.1. Các đặc trưng của một hệ mật mã

- Kiểu của các thao tác mã hoá được sử dụng:
  - phép thế
  - thay đổi vị trí (hoán vị)
  - tích của chúng.
- Số khoá được sử dụng:
  - Khoá duy nhất (khóa đối xứng – hệ mật mã khóa bí mật)
  - Hai khoá (khóa không đối xứng – hệ mật mã khóa công khai)

3.2. Các đặc trưng của một hệ mật mã (tiếp)

- Cách mà bản rõ được xử lý:
  - Khối:
    - Bản rõ được chia thành nhiều khối có kích thước xác định (64 bít, 128 bít)
    - Áp dụng thuật toán mã hóa cho từng khối
    - DES (Data encryption standard - 1977)
  - Dòng bít:
    - Xử lý từng đơn vị thông tin đầu vào (bít hoặc byte)
    - Độ dài khóa = độ dài bản rõ
    - Bộ đêm 1 lần (One time pad)

3.3. An toàn của một hệ mã

- **An toàn không điều kiện**: không quan trọng máy tính mạnh như thế nào, mã hoá không thể bị bẻ vì bản mã không cung cấp đủ thông tin để xác định duy nhất bản rõ.

  => Thuật toán dùng bộ đệm một lần

- **An toàn tính toán**:
  - giá để phá hệ mã vượt quá giá trị của thông tin
  - thời gian để bẻ mã vượt quá thời gian có ích của thông tin
- => An toàn tính toán được coi là an toàn

3.4. Tấn công một hệ mật mã

- Mục đích là tìm khoá chứ không phải tìm bản tin cụ thể (bản rõ)

- Có các cách :
  - *tấn công thám mã (cryptanalysis)*: dựa vào thuật toán mã hóa đã biết và những thông tin hoặc đặc trưng về cặp đôi "bản rõ – bản mã hóa"
  - *tìm duyệt toàn bộ (brute-force):* cố gắng thử mọi khả năng của "khóa" để tìm được bản rõ tốt nhất.
    - trung bình phải thử hơn nửa số khóa

3.5. Các cách tiếp cận để thám mã

1. **Chỉ dùng bản mã**: biết thuật toán và bản mã

   => dùng phương pháp thống kê, xác định bản rõ.

2. **Biết bản rõ**: biết thuật toán, biết ít nhất một cặp bản mã/bản rõ để tấn công mã
3. **Bản rõ được chọn**: biết thuật toán, biết bản mã, kẻ tấn công tự chọn một đoạn tin bản rõ mà đã có được bản mã tương ứng. (đoạn tin bản rõ: phần đầu của hóa đơn)
4. **Bản mã được chọn**: biết thuật toán, biết bản mã, kẻ tấn công chọn bản mã cùng với bản rõ đã được giải mã tương ứng
5. **Văn bản được chọn**: gồm cả 3 và 4

   =>1,2,3 thường được dùng để thám mã

3.6. Tìm duyệt - Brute Force Search

- Thử từng khóa
- Trung bình phải thử một nửa số khóa

=> DES ko đảm bảo độ an toàn tính toán

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/μs	Time required at 10^6 decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56 (DES)	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128 (AES)	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168 (Triple DES)	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

Nội dung

1. Tổng quan về mã cổ điển
2. Mã đối xứng và các khái niệm cơ bản
3. Các đặc trưng của một hệ mật mã
4. Mã thế
5. Mã hoán vị
6. Mã tích

4.1. Mã thế (cổ điển)
(Classical Substitution Ciphers)

- Ở đây các chữ của bản rõ được thay bằng các chữ khác hoặc các số hoặc các ký hiệu.
- Hoặc nếu xem bản rõ như môt dãy bít, thì phép thế thay các mẫu bít bản rõ bằng các mẫu bít bản mã
- Các loại mã thế cổ điển: Ceasar, Playfair, Vigenere…

4.2. Mã Ceasar

- Mã thế được biết sớm nhất
- Được sáng tạo bởi Julius Ceasar
- Đầu tiên được sử dụng trong quân sự
- Thay mỗi chữ bằng chữ thứ ba tiếp theo trong bảng chữ cái
- Ví dụ:

```
meet me after the toga party
=> PHHW PH DIWHU WKH WRJD SDUWB
```

4.2. Mã Caesar (tiếp)

- Có thể định nghĩ qua phép dịch chuyển

```
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
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
```

- Về toán học, nếu gán số cho mỗi chữ

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

- thì mã Ceasar được định nghĩa như sau

$c = E(p) = (p + k) \bmod (26)$

$p = D(c) = (c - k) \bmod (26)$

p: số thứ tự của chữ trong bản rõ
c: số thứ tự của chữ trong bản mã
k: số bước tịnh tiến các chữ (khóa của mã Ceasar)

4.3. Thám mã Ceasar

- Chỉ có 26 khoá có thể:
  - A ánh xạ vào A, B, C, …, Z
  - Cần 5 bit để biểu diễn khóa
- Thám mã đơn giản: Có thể thử lần lượt
- Sử dụng tìm duyệt
- Cho bản mã, hãy thử mọi cách dịch chuyển các chữ
- Đoán nhận thông qua nội dung các bản rõ nhận được
- Ví dụ: bẻ bản mã "GCUA VQ DTGCM" cho "easy to break". bước tịnh tiến là 24

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	ydrcp	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
11	ewwl	ew	sxlwj	lzw	lgys	hsjlq
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	zrrg	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	glzkx	znk	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

4.4. Mã bảng chữ đơn

- Không chỉ là dịch chuyển bảng chữ
- Có thể tạo các bước nhảy các chữ tùy ý
- Mỗi chữ của bản rõ được ánh xạ đến một chữ ngẫu nhiên khác nhau của bản mã => một khóa tương ứng với 1 hoán vị của 26 chữ cái
- Như vậy độ dài khoá là 26
- Ví dụ:
- Plain: abcdefghijklmnopqrstuvwxyz
- Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN
- Plaintext: ifwewishtoreplaceletters
- Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

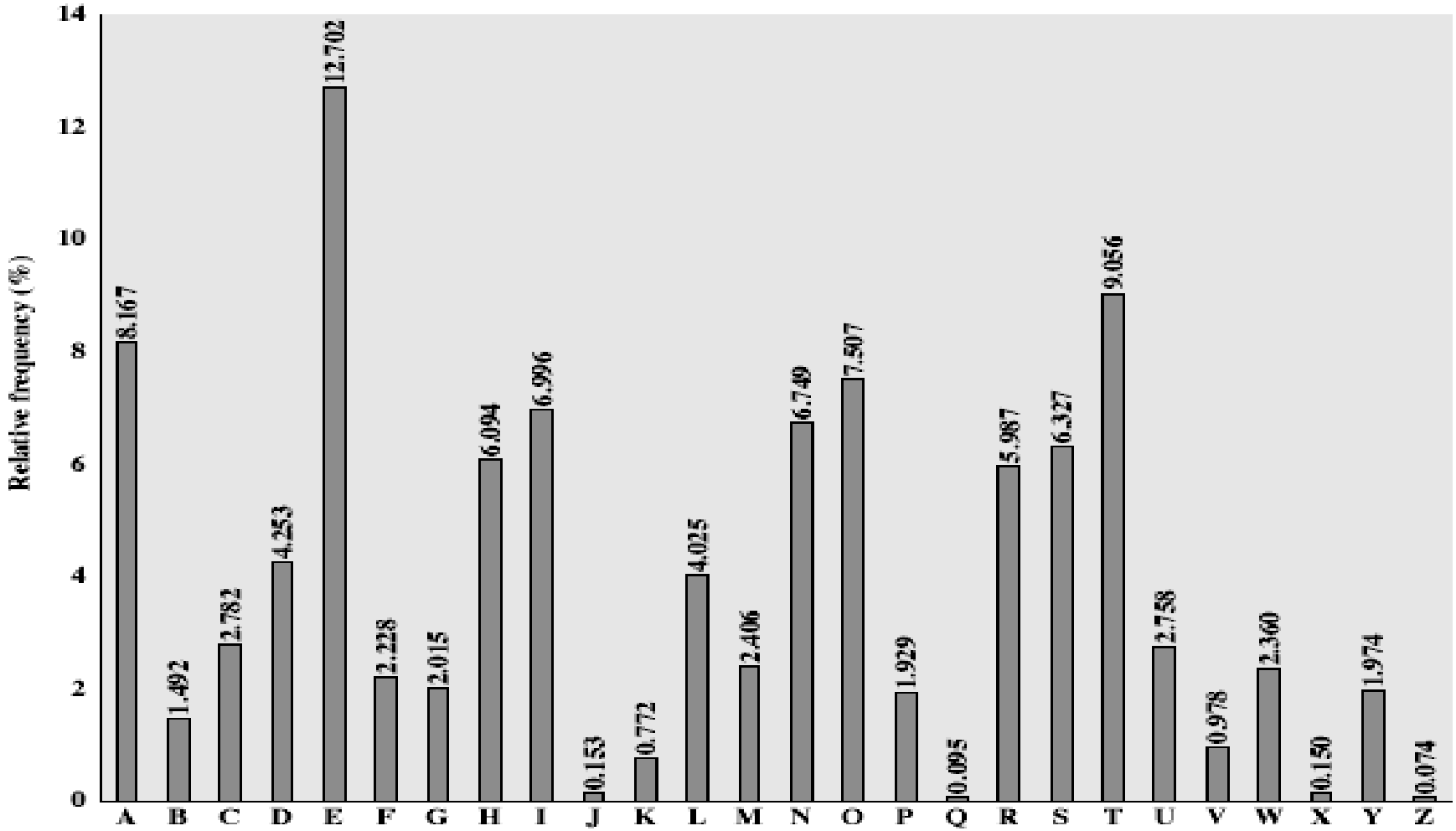
4.5. Tính an toàn của mã trên bảng chữ đơn

- Tổng cộng có 26! ~ 4 x 10^{26} khoá
- Với khá nhiều khoá như vậy nhiều người nghĩ là an toàn
- Nhưng không phải như vậy: Sai!!!
- Vấn đề ở đây là do các đặc trưng về ngôn ngữ =>dựa vào tần suất xuất hiện của các chữ để bẻ mã

4.6. Một số đặc tính của ngôn ngữ giúp ích cho thám mã bảng chữ đơn

- Các chữ không được sử dụng thường xuyên như nhau
- Trong tiếng Anh chữ E được sử dụng nhiều nhất
- Sau đó đến T,R,N,I,O,A,S
- Một số chữ rất ít dùng như: Z,J,K,Q,X
- Có bảng các tần suất các chữ đơn, cặp chữ (th, no…), bộ ba chữ (ful, rst…).

4.7. Bảng tần suất chữ cái tiếng Anh
English Letter Frequencies



4.8. Thám mã bảng chữ đơn

- Điều quan trọng là mã thế trên bảng chữ đơn không làm thay đổi tần suất tương đối của các chữ.
- Được phát hiện bởi các nhà khoa học Ai cập từ thế kỷ thứ 9.
- Tính toán tần suất của các chữ trong bản mã
- So sánh với các giá trị đã biết
- Tìm kiếm các chữ đơn hay dùng A-I-E, bộ đôi NO và bộ ba RST; và các bộ ít dùng JK, X-Z..
- Trên bảng chữ đơn cần xác định các chữ, dùng các bảng bộ đôi và bộ ba trợ giúp.

4.9. Ví dụ thám mã bảng chữ đơn

- Cho bản mã:

  UZQSOVUOHXMOPVGPOZPEVSG**ZW**ZSZOPFPESXUDBMETSXAI
  ZVUEPHZHMDZSHZOWSFPAPPDTSVPQU**ZW**YMXUZUHSXEPYE
  POPDZSZUFPOMB**ZW**PFUPZHMDJUDTMOHMQ

- Thám mã
  - Tính tần suất các chữ
  - Đoán P và Z là e và t.
  - Khi đó ZW là th và ZWP là the.
  - Suy luận tiếp tục ta có:

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

4.10. Mã Playfair

- Không phải số khoá lớn trong mã bảng chữ đơn đảm bảo an toàn mã.
- Một hướng khắc phục là **mã bộ các chữ:** mỗi chữ được mã bằng một số chữ khác nhau.
- Playfair là một trong các mã như vậy, mỗi chữ có thể được mã hóa bởi 7 chữ khác nhau
- Được sáng tạo bởi Charles Wheastone 1854 và mang tên người bạn là Baron Playfair

4.11. Ma trận khoá Playfair

- Chọn 1 từ làm khóa (ko lặp chữ cái)
- Là ma trận gồm các chữ cỡ 5 x 5 dựa trên một từ khoá, theo quy tắc:
  - Viết các chữ của từ khoá vào ma trận (từ hàng đầu)
  - nếu còn trống, viết các chữ khác vào các ô còn lại theo một thứ tự nhất định
- Chẳng hạn sử dụng từ khóa MONARCHY

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

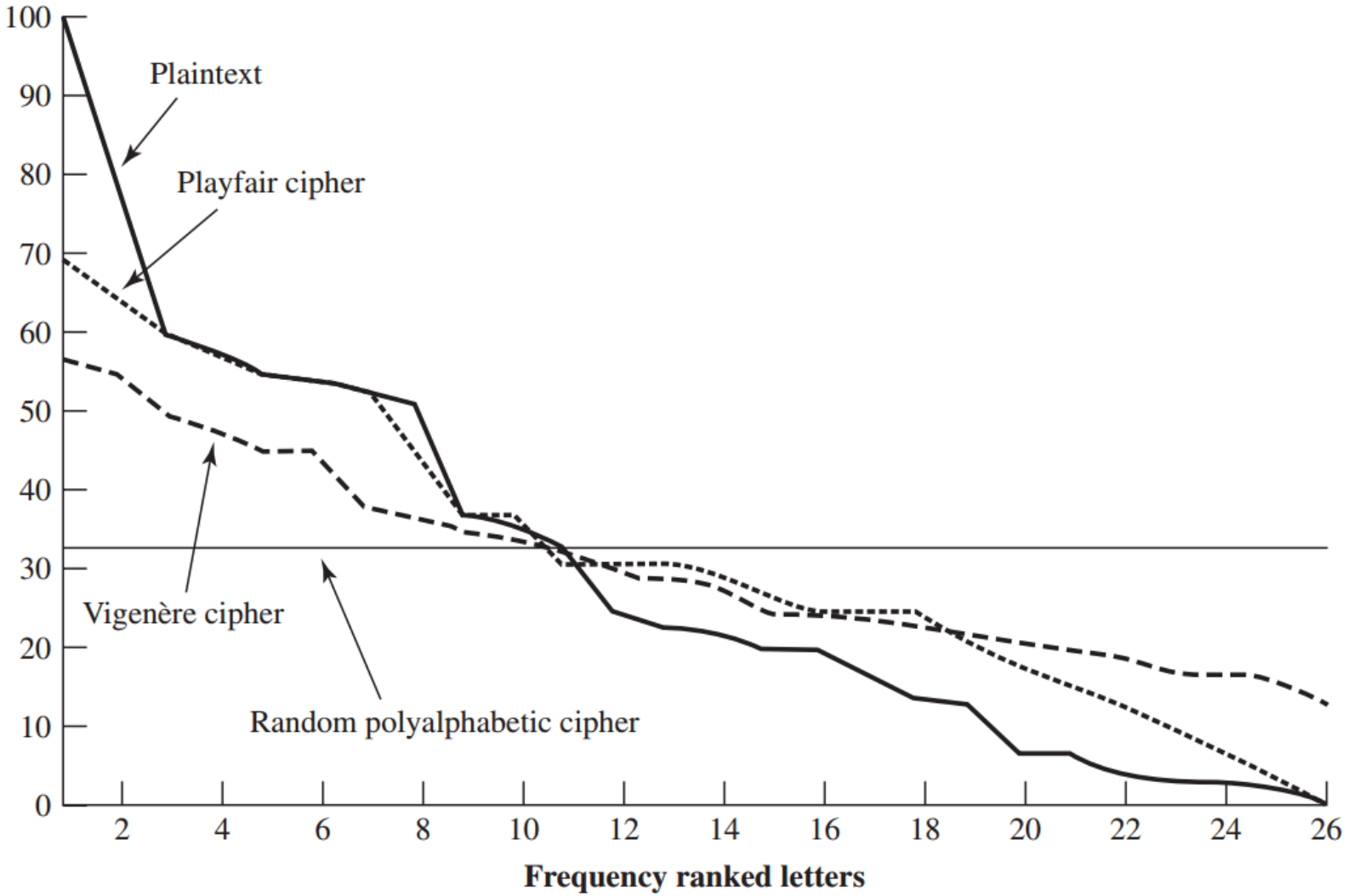
4.12. Quy tắc mã hoá Playfair

- bản rõ được mã hoá cặp 2 chữ kề nhau cùng một lúc
  - Nếu một cặp nào đó là chữ lặp, thì chèn thêm một từ lọc chẳng hạn X. Ví dụ, trước khi mã **“balloon”** biến đổi thành **“ba lx lo on”**
  - Nếu cả hai chữ đều rơi vào cùng một hàng, thì mã mỗi chữ bằng chữ ở phía bên phải nó (cuộn vòng quanh từ cuối về đầu), chẳng hạn “**ar”** biến đổi thành “RM”
  - Nếu cả hai chữ đều rơi vào cùng một cột, thì mã mỗi chữ bằng chữ ở phía bên dưới nó (cuộn vòng quanh từ cuối về đầu), chẳng hạn “**mu”** biến đổi thành “CM”
  - Trong các trường hợp khác, mỗi chữ được mã bởi chữ cùng hàng với nó và cùng cột với chữ cùng cặp với nó. Chẳng hạn, **“hs”** mã thành **“BP”**, và **“ea”** mã thành **“IM”** hoặc **“JM”** (tuỳ theo sở thích)

4.13. An toàn của mã Playfair

- An toàn được nâng cao so với bảng đơn
- Vì có 26 x 26 = 676 cặp
- Cần phải có bảng tần suất của 676 cặp để thám mã (so với 26 của mã bảng đơn)
- Và tương ứng sẽ nhiều bản mã hơn.
- Được sử dụng rộng rãi trong nhiều năm trong giới quân sự Mỹ và Anh (trong chiến tranh thế giới thứ 1)
- Nó có thể bị bẻ khoá nếu cho trước vài trăm chữ vì bản mã còn chứa nhiều cấu trúc của bản rõ.

4.14. Tần suất xuất hiện của các chữ cái



4.15. Mã hóa đa bảng

- Dùng nhiều bảng ký tự mã hóa cho một bản rõ
- Tần suất các chữ trong bản mã được trải bằng => không mang nhiều cấu trúc của bản rõ
- Sử dụng khoá để chọn bảng nào được dùng cho từng chữ trong bản tin
- Số bảng chữ cái = độ dài khóa
- Sử dụng lặp lại các bảng để mã hóa cho bản rõ

4.16. Mã Vigenere

- Là mã thế đa bảng đơn giản nhất
- Hiệu quả như dùng nhiều mã Ceasar cùng một lúc
- Khoá là một dãy các ký tự có độ dài K = K1K2…Kd
- Chữ thứ i chỉ định dùng bảng chữ thứ i với tịnh tiến tương ứng ký tự Ki
- Chia bản rõ thành các khối d ký tự
- Lặp lại từ đầu sau d ký tự của bản rõ
- Giải mã đơn giản là làm việc ngược lại.

4.17. Ví dụ dùng mã Vigenère

```
key:          deceptivedeceptivedeceptive
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

- Về mặt toán học:

key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

4.18. Mã Vigenere (tiếp)

- Plain text: P = $p_0, p_1, \ldots, p_{n-1}$
- Key: K = $k_0, k_1, \ldots, k_{m-1}$ (m<n)
- Cipher text: C = $C_0, C_1, \ldots, C_{n-1}$

$$C = C_0, C_1, C_2, \ldots, C_{n-1} = \mathrm{E}(K, P) = \mathrm{E}[(k_0, k_1, k_2, \ldots, k_{m-1}), (p_0, p_1, p_2, \ldots, p_{n-1})]$$
$$= (p_0 + k_0) \bmod 26, (p_1 + k_1) \bmod 26, \ldots, (p_{m-1} + k_{m-1}) \bmod 26,$$
$$(p_m + k_0) \bmod 26, (p_{m+1} + k_1) \bmod 26, \ldots, (p_{2m-1} + k_{m-1}) \bmod 26, \ldots$$

$\Rightarrow$Mã hóa $$C_i = (p_i + k_{i \bmod m}) \bmod 26$$

$\Rightarrow$Giải mã $$p_i = (C_i - k_{i \bmod m}) \bmod 26$$

4.19. An toàn của mã Vigenere

- Ưu điểm:
  - Có chữ mã khác nhau cho cùng chữ của bản rõ
  - Suy ra tần suất của các chữ khá đều
- Yếu điểm
  - Bắt đầu từ tần suất của chữ => Mã đơn bảng hay mã đa bảng?
  - Độ dài khóa có hạn nên có thể tạo chu kỳ vòng lặp

  =>Xác định số bảng chữ và lần tìm từng chữ
- Nên tăng độ dài khóa

4.20. Thám mã Vigenere

```
key:          deceptivedeceptivedeceptive
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

- Đề xuất bởi Babbage (sau hàng thế kỷ)
  - Xác định độ dài của khóa:
    - Tìm chuỗi được lặp lại trong bản mã
    - Độ dài khoảng lặp là bội số của chiều dài khóa

    $\Rightarrow$Nếu có nhiều khoảng lặp sẽ dễ tìm được độ dài khóa
    - Giả sử độ dài khóa là m => bản mã sử dụng m bảng mã đơn
    - Các ký tự ở các vị trí 1, m+1, 2m+1…trong bản mã sẽ dung chung 1 bảng mã đơn
    - Dùng tần suất xuất hiện ký tự trong văn bản để thám mã trên từng bảng mã đơn

4.21. Mã khoá tự động-Autokey Cipher

- Lý tưởng có khoá dài như bản tin
- Vigenere đề xuất khoá tự động
- Với từ khoá được nối vào đầu bản tin tạo thành khoá
- Biết từ khoá có thể khôi phục được một số chữ ban đầu
- Tiếp tục sử dụng chúng cho văn bản còn lại
- Nhưng vẫn còn đặc trưng tần suất để tấn công
- Ví dụ: cho từ khoá **deceptive**

key: deceptivewearediscoveredsav
plaintext: wearediscoveredsaveyourself
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA

4.22. Bộ đệm một lần (One-Time Pad)

- Nếu khoá thực sự ngẫu nhiên có độ dài bằng bản rõ được dùng, thì mã hoá sẽ an toàn

=>Gọi là bộ đệm một lần

- Sẽ không bẻ được vì bản mã không có liên quan thống kê gì với bản rõ.
  - Vì với bản rõ bất kỳ và bản mã bất kỳ, luôn tồn tại một khoá để ánh xạ bản rõ đó sang bản mã đã cho.
- Khó khăn: sinh và phân phối an toàn khoá.

Nội dung

1. Tổng quan về mã cổ điển
2. Mã đối xứng và các khái niệm cơ bản
3. Các đặc trưng của một hệ mật mã
4. Mã thế
5. Mã hoán vị
6. Mã tích

5.1. Các mã hoán vị đổi chỗ

- Chỉ thay đổi vị trí các ký tự trong bản rõ
- Không thay đổi các chữ thực tế được dùng

=> Có thể nhận biết được vì bản mã có cùng phân bố tần suất như bản gốc.

5.2. Mã Rail Fence

- Viết các chữ của bản tin theo đường zíc zắc trên một số dòng, số dòng chính là khóa của mã
- Sau đó đọc theo từng dòng để nhận được bản mã
- Ví dụ: viết bản tin “meet me after the toga party” như sau (khóa k=2)

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

e t e f e t e o a a t

=>cho bản mã:

MEMATRHTGPRYETEFETEOAAT

5.3. Mã dịch chuyển dòng

- Viết các chữ của bản tin theo các dòng trên số cột xác định
- Sau đó thay đổi thứ tự các cột theo một khoá trước khi đọc lại chúng theo cột
- Ví dụ: “attack postponed until two am”

Key:	4	3	1	2	5	6	7
Plaintext:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Nội dung

1. Tổng quan về mã cổ điển
2. Mã đối xứng và các khái niệm cơ bản
3. Các đặc trưng của một hệ mật mã
4. Mã thế
5. Mã hoán vị
6. Mã tích

6.1. Mã tích

- Mã dùng hoán vị hoặc dịch chuyển không an toàn vì các đặc trưng của ngôn ngữ
- Vì vậy sử dụng một số mã liên tiếp sẽ làm cho mã khó hơn, nhưng
  - Tích hai hoán vị sẽ tạo nên hoán vị phức tạp hơn
  - Tich hai phép thế tạo nên phép thế phức tạp hơn

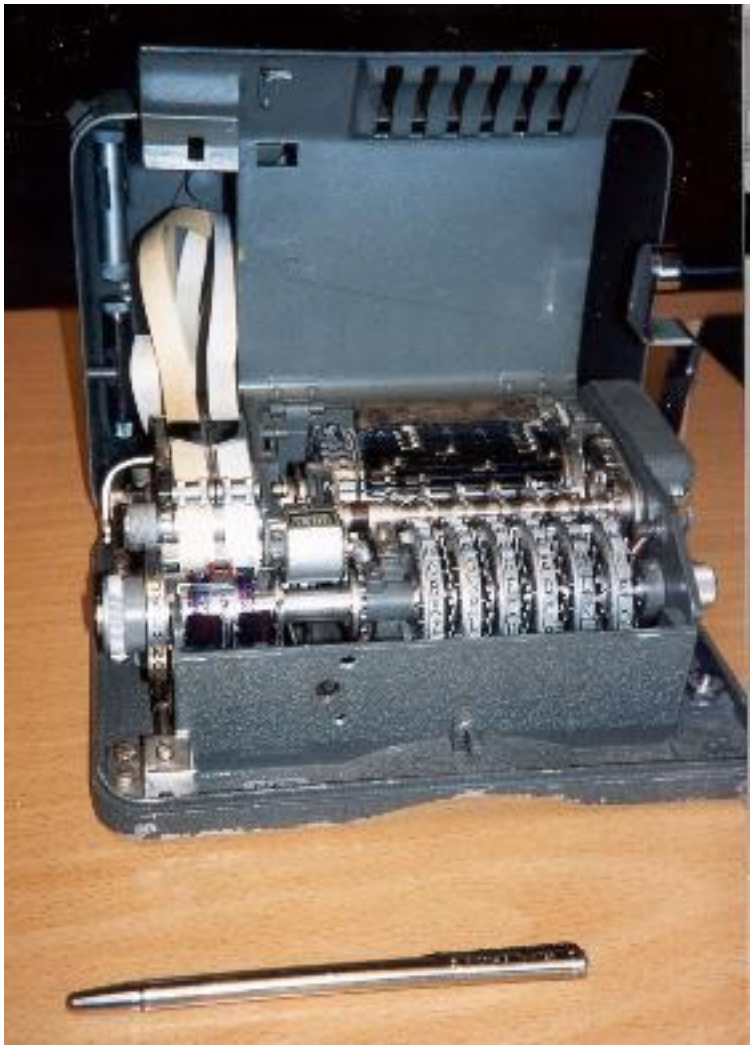
=>Mã tích: Phép thế được nối tiếp bằng phép dịch chuyển tạo nên mã mới khó hơn rất nhiều

- Đây là chiếc cầu từ cổ điển sang hiện đại

6.2. Máy quay

- Trước khi có mã hiện đại, máy quay là mã tích thông dụng nhất
- Được sử dụng rộng rãi trong chiến tranh thế giới thứ hai: Đức, đồng minh và Nhật
- Tạo nên mã thế rất đa dạng và phức tạp
- Sử dụng một số lõi hình trụ, mỗi lõi ứng với một phép thế, khi quay sẽ thay đổi sau khi mỗi chữ được mã.
  - Với 3 hình trụ có 26 x 26 x 26 = 17576 bảng chữ
- Là tiền đề phát triển thuật toán DES

Hagelin Rotor Machine



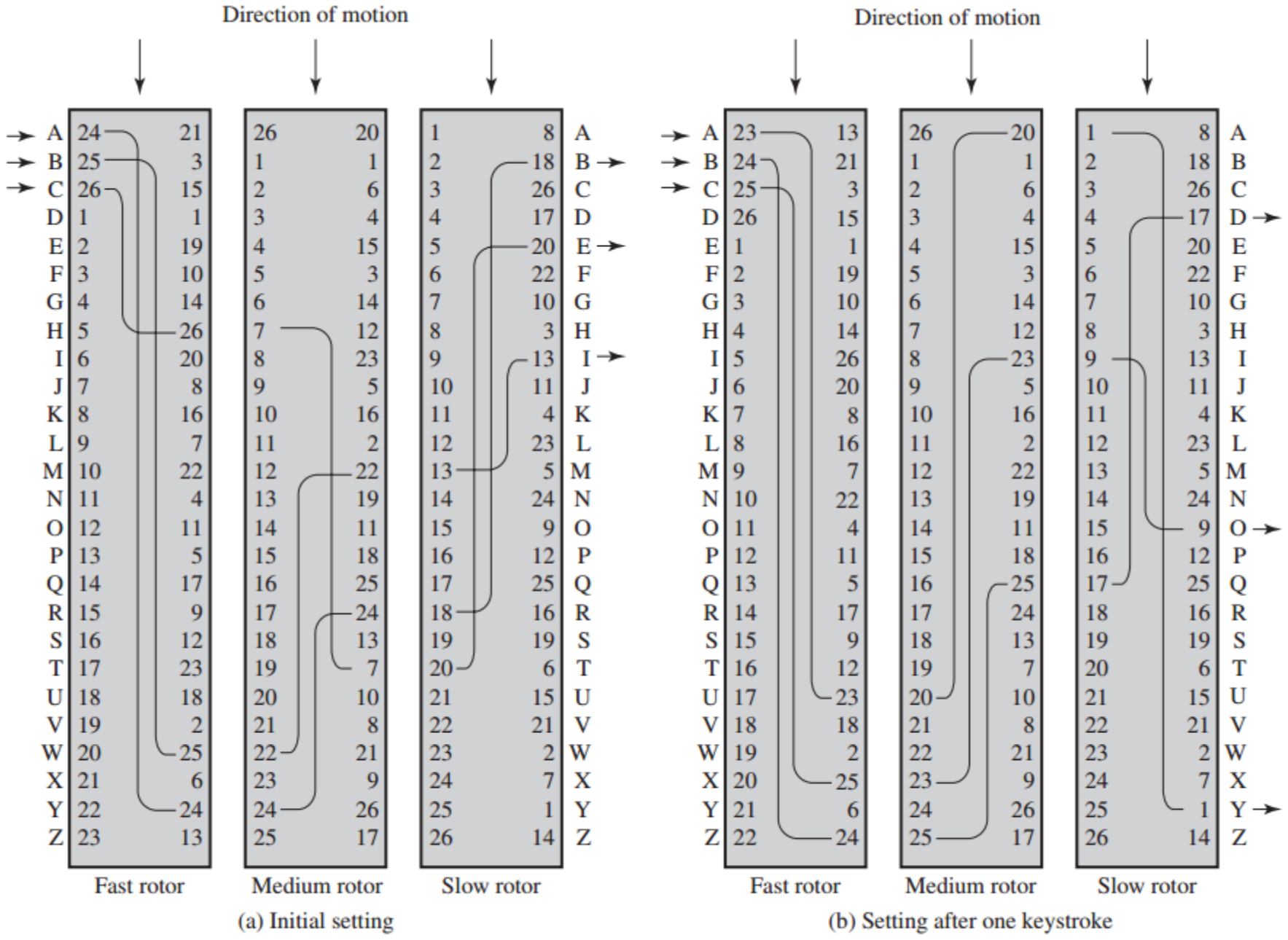


Figure 2.8 Three-Rotor Machine with Wiring Represented by Numbered Contacts

Kết luận - Summary

- Đã xét:
  - Các thuật ngữ và kỹ thuật mã cổ điển
  - Các mã thế đơn bảng chữ
  - Thám mã sử dụng tần suất của các chữ
  - Mã Playfair
  - Mã thế đa bảng chữ
  - Bộ đêm 1 lần
  - Mã hoán vị (đổi chỗ)
  - Tích các mã và máy quay