

Lecture 3

Classical Encryption Techniques

Jason Lin

Outline

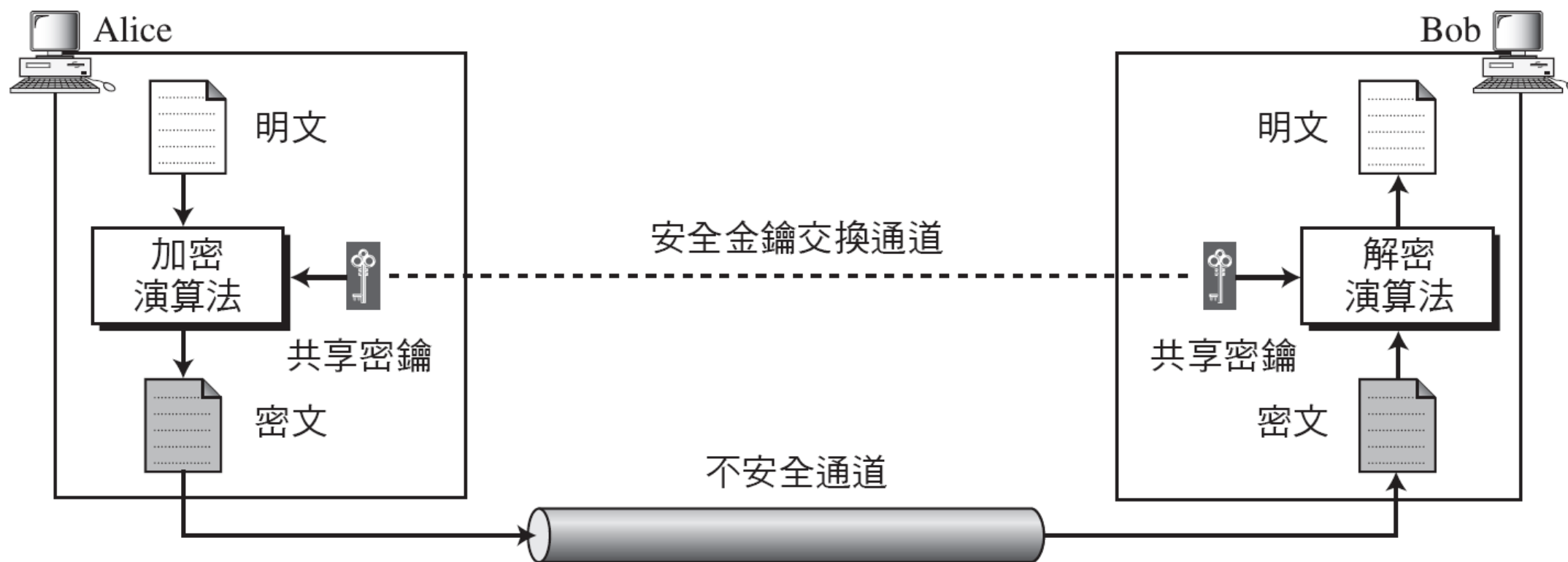
- Symmetric Encryption
- Techniques of Classical Ciphers
- Stream and Block Ciphers

Symmetric Encryption (1/2)

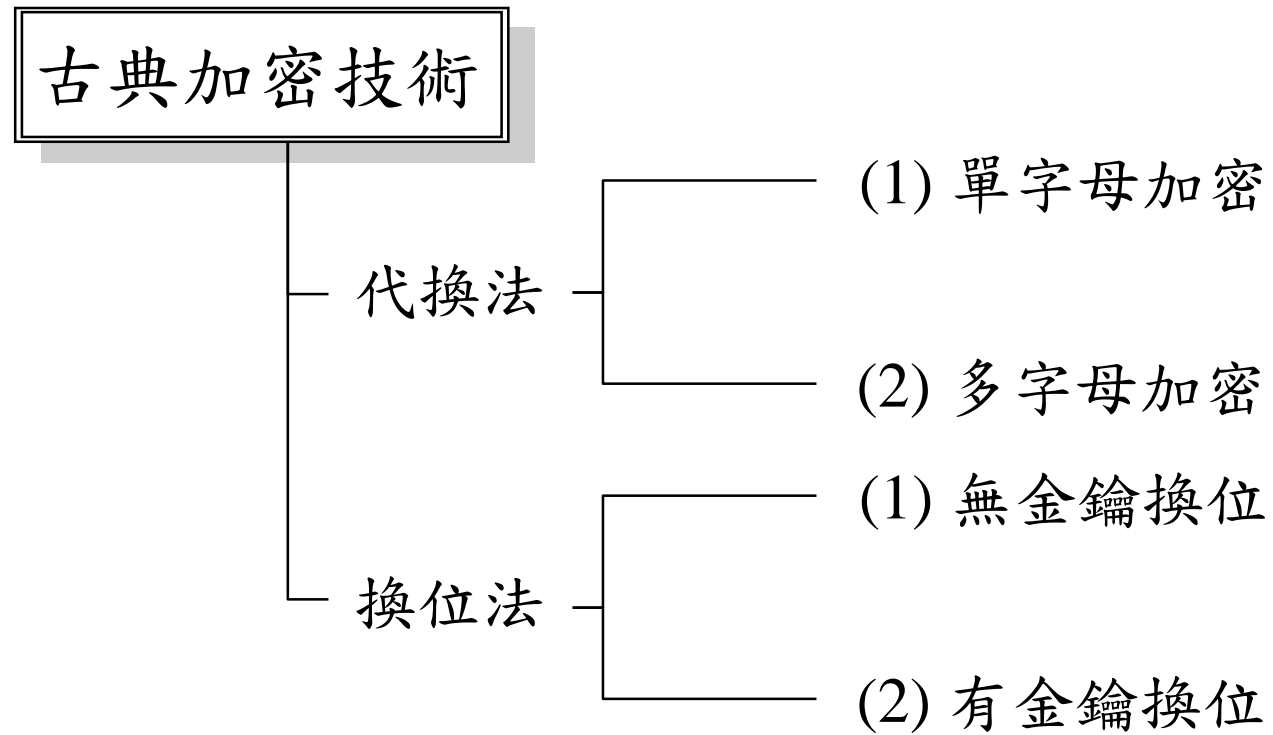
- 對稱式金鑰 (Symmetric Key)：以同一把金鑰來加密或解密



Symmetric Encryption (2/2)

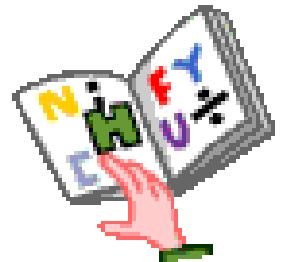


Techniques of Classical Ciphers



Substitution Techniques

- Substitution Techniques (代換法)
 - Is one in which the letters of plaintext are replaced by other letters or by numbers or symbols
 - If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns
- There are two types of substitution techniques
 - Monoalphabetic ciphers (單字母加密法)
 - Polyalphabetic ciphers (多字母加密法)



Monoalphabetic Cipher (1/2)

- 在單字母加密法 (Monoalphabetic Cipher) 中，明文裡的符號和密文的符號通常都是一對一取代的。
- 下面顯示的是明文和其對應的密文，明文用小寫字體，密文則用大寫字體。這很可能為單字母加密法，因為兩個 l 在轉換為密碼時都變成了 O。

明文：hello

密文：KHOOR

- 下面顯示明文和其對應的密文，這就不是單字母加密法，因為每個 l 轉換成密碼時都變成不同的字，第一個變成 N，第二個變成 Z。

明文：hello

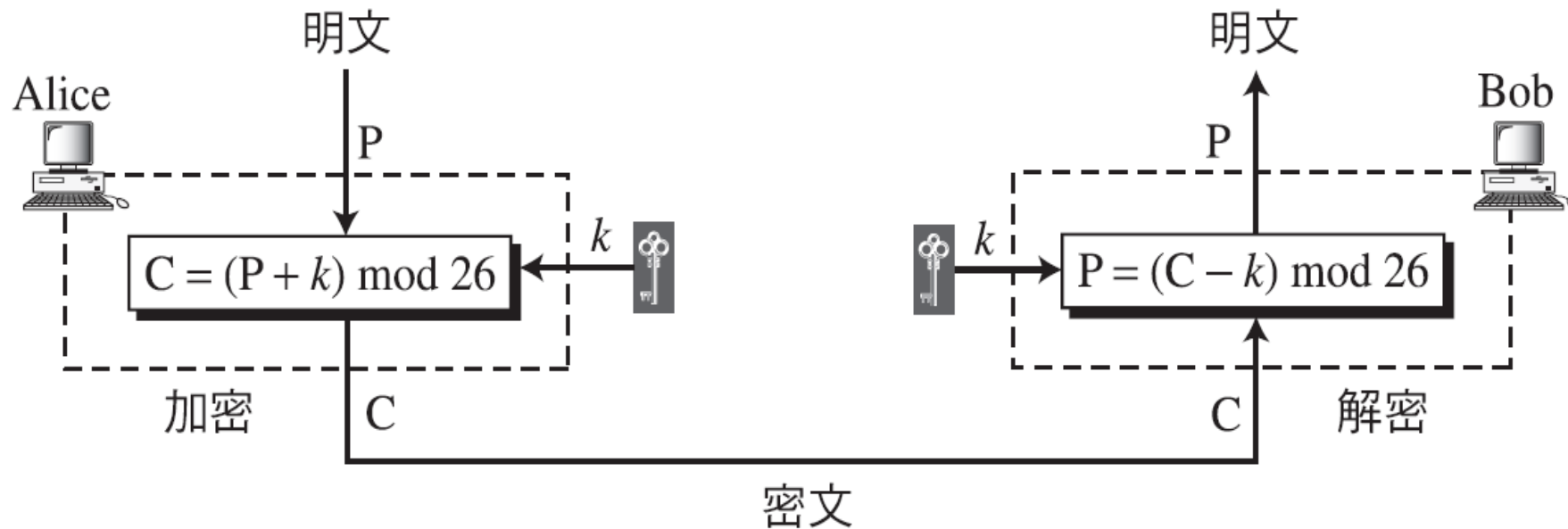
密文：ABNZF

Monoalphabetic Cipher (2/2)

- 最簡單的單字母加密法就是加法加密法 (Additive Cipher)。此加密法有時稱為位移加密法 (Shift Cipher)。
- 因為 Julius Ceasar 以 3 當成金鑰，利用加法加密法與他的下屬聯繫，因此加法加密法有時亦稱為凱撒加密法 (Caesar Cipher)，但加法加密法比較能顯示出其數學意涵。

Caesar Cipher (1/5)

- 因為是加法加密法，所以其明文、密文和金鑰都是 Z_{26} 中的整數。



Caesar Cipher (2/5)

- Z_{26} 中表示明文和密文字母的數

明文	→	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
密文	→	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
值	→	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Caesar Cipher (3/5)



- 凱撒加密法：25種可能的金鑰（取 $k = 3$ ）
 - $f(a) = (a + k) \bmod n$
 - a = 該字在字集中原先位置； k = 移動的位置； n = 此字集的大小。

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

Plaintext: secure all messages

Ciphertext: VHFXUH DOO PHVVDJHV

$$C = E(P) = (P + k) \bmod (26) = (P + 3) \bmod (26)$$

$$P = D(C) = (C - k) \bmod (26) = (C - 3) \bmod (26)$$

Caesar Cipher (4/5)

- 使用加法加密法，以金鑰 = 15 加密訊息「hello」。
- 解法：我們以字對字的方式應用加密演算法於明文。

明文：h→ 07	加密： $(07 + 15) \bmod 26$	密文：22→ W
明文：e→ 04	加密： $(04 + 15) \bmod 26$	密文：19→ T
明文：l→ 11	加密： $(11 + 15) \bmod 26$	密文：00→ A
明文：l→ 11	加密： $(11 + 15) \bmod 26$	密文：00→ A
明文：o→ 14	加密： $(14 + 15) \bmod 26$	密文：03→ D

Caesar Cipher (5/5)

- 使用加法加密法，以金鑰 = 15 解密訊息「WTAAD」。
- 解法：我們以字對字的方式應用解密演算法於明文。

密文：W → 22

解密： $(22 - 15) \bmod 26$

明文：07 → h

密文：T → 19

解密： $(19 - 15) \bmod 26$

明文：04 → e

密文：A → 00

解密： $(00 - 15) \bmod 26$

明文：11 → l

密文：A → 00

解密： $(00 - 15) \bmod 26$

明文：11 → l

密文：D → 03

解密： $(03 - 15) \bmod 26$

明文：14 → o

Brute-Force Cryptanalysis

- Three important characteristics of Caesar cipher:
 - The encryption and decryption algorithms are known.
 - There are only 25 keys to try.
 - The language of the plaintext is known and easily recognizable.



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	rfe	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	hsjlq
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	putg	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	rjyy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

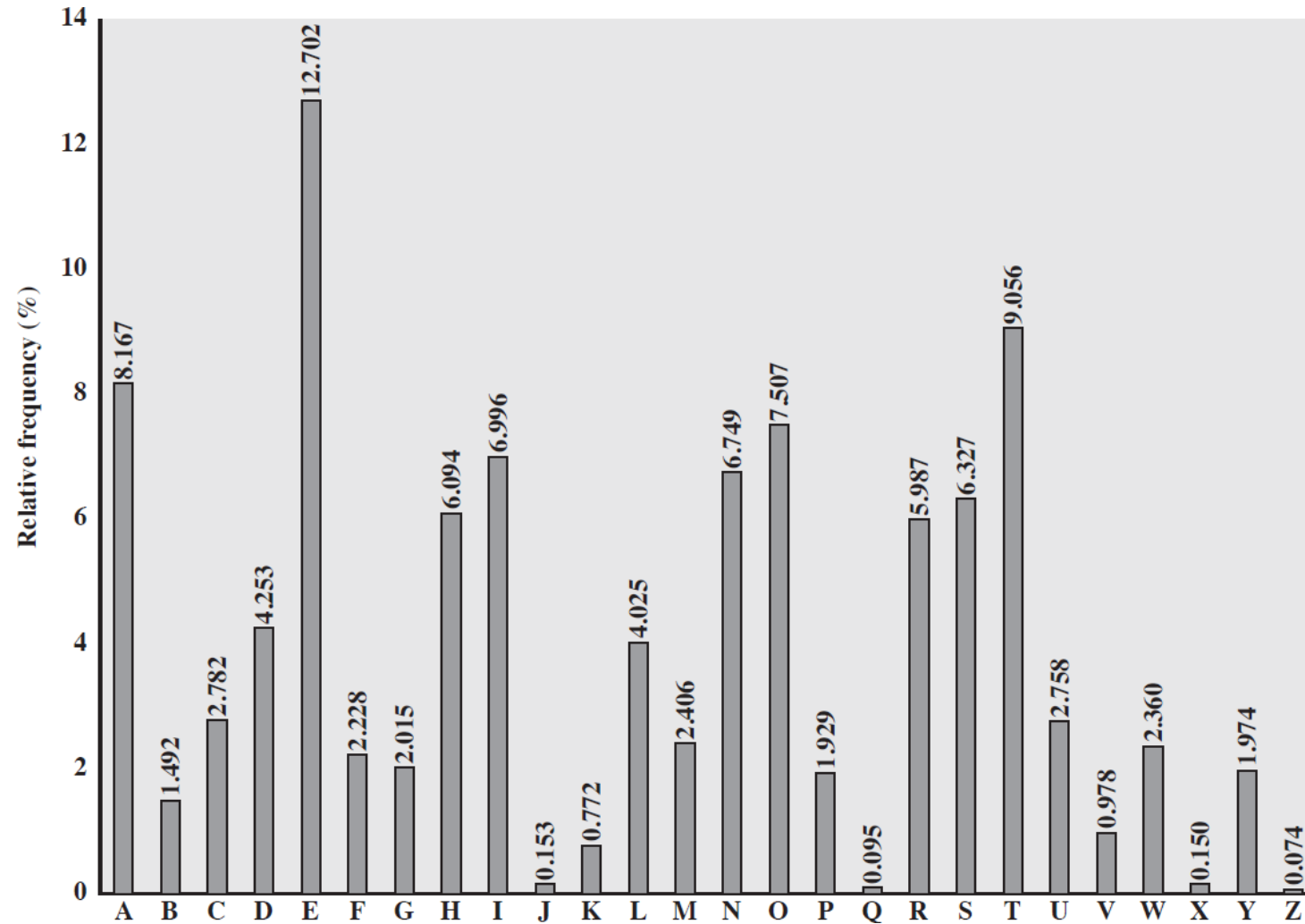
An Example of Brute-Force Cryptanalysis

- Eve 已截取的密文「UVACLYFZLJBYL」。證明她如何使用暴力攻擊破解加密法。

密文：UVACLYFZLJBYL

K = 1	→	明文：tuzbkxeykiaxk
K = 2	→	明文：styajwdxjhzwj
K = 3	→	明文：rsxzivcwigyvi
K = 4	→	明文：qrwyhubvhfxuh
K = 5	→	明文：pqvxgtaugewtg
K = 6	→	明文：opuwfsztfdvsvf
K = 7	→	明文：notverysecure

Statistical Cryptanalysis



An Example of Statistical Cryptanalysis (1/2)

- 假設英文字母出現的頻率如下表

字母	頻率	字母	頻率	字母	頻率	字母	頻率
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

An Example of Statistical Cryptanalysis (2/2)

- Eve 攔截了以下密文，並用統計攻擊找到明文。

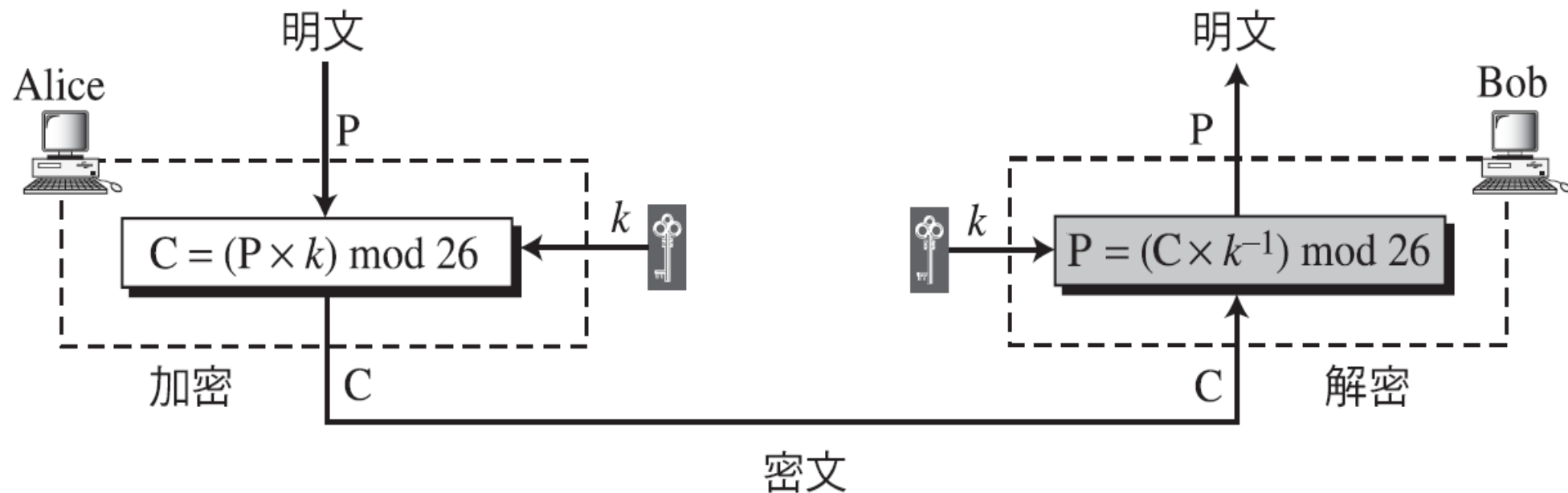
XLILSYWIMWRS AJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVXLQSVILY-
VVCFIJSVIXLIWIPPIVVIGIMZIWQSVISJJIVW

- 解法：當 Eve 將密文中字母出現的頻率列表顯示時，她得到：I = 14，V = 13，S = 12等。最常出現的字母是 I，頻率為14次，顯示 I 有可能對應明文中的字此 e，並表示金鑰 = 4。

the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers

Multiplicative Cipher (1/2)

- 在乘法加密法 (Multiplicative Cipher) 中，明文和密文都是 Z_{26} 的整數；金鑰為一個 Z_{26}^* 的整數。



Multiplicative Cipher (2/2)

- 乘法加密法的金鑰範圍為何？
- 解法：金鑰必須在 Z_{26}^* 之內，此組合只有12個：1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25。
- 我們使用乘法加密法和金鑰 7 加密訊息「hello」，其密文為「XCZZU」。

明文：h → 07

加密： $(07 \times 07) \bmod 26$

密文：23 → X

明文：e → 04

加密： $(04 \times 07) \bmod 26$

密文：02 → C

明文：l → 11

加密： $(11 \times 07) \bmod 26$

密文：25 → Z

明文：l → 11

加密： $(11 \times 07) \bmod 26$

密文：25 → Z

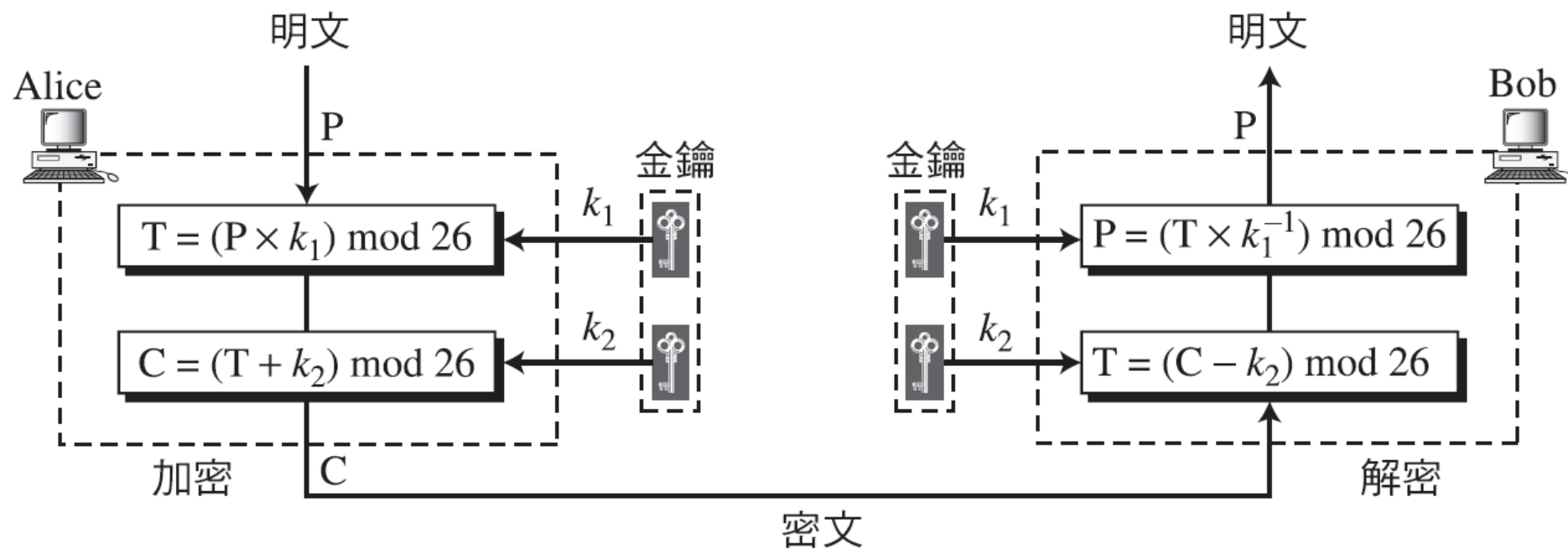
明文：o → 14

加密： $(14 \times 07) \bmod 26$

密文：20 → U

Affine Cipher (1/4)

- 仿射加密法 (Affine Cipher) 使用一對金鑰，第一把出自 Z_{26}^* ，而第二把出自 Z_{26} 。其金鑰範圍大小為 $12 \times 26 = 312$ 。



Affine Cipher (2/4)

- 仿射加密法的加解密定義如下

$$C = (P \times k_1 + k_2) \bmod 26 \quad P = ((C - k_2) \times k_1^{-1}) \bmod 26$$

其中， k_1^{-1} 是 k_1 的乘法反元素，而 $-k_2$ 是 k_2 的加法反元素

- 加法加密法可視為仿射加密法裡當 $k_1 = 1$ 時的特例，而乘法加密法為 $k_2 = 0$ 時的特例。

Affine Cipher (3/4)

- 使用仿射加密法及金鑰對 $(7, 2)$ 加密訊息「hello」。
- 解法

明文：h→07	加密： $(07 \times 07 + 2) \bmod 26$	密文：25→Z
明文：e→04	加密： $(04 \times 07 + 2) \bmod 26$	密文：05→E
明文：l→11	加密： $(11 \times 07 + 2) \bmod 26$	密文：01→B
明文：l→11	加密： $(11 \times 07 + 2) \bmod 26$	密文：01→B
明文：o→14	加密： $(14 \times 07 + 2) \bmod 26$	密文：22→W

Affine Cipher (4/4)

- 使用仿射加密法及模數 26 裡的金鑰對 (7, 2) 解密訊息「ZEBBW」。
- 解法

密文：Z \rightarrow 25	解密： $((25 - 2) \times 7^{-1}) \bmod 26$	明文：07 \rightarrow h
密文：E \rightarrow 04	解密： $((04 - 2) \times 7^{-1}) \bmod 26$	明文：04 \rightarrow e
密文：B \rightarrow 01	解密： $((01 - 2) \times 7^{-1}) \bmod 26$	明文：11 \rightarrow l
密文：B \rightarrow 01	解密： $((01 - 2) \times 7^{-1}) \bmod 26$	明文：11 \rightarrow l
密文：W \rightarrow 22	解密： $((22 - 2) \times 7^{-1}) \bmod 26$	明文：14 \rightarrow o

Monoalphabetic Substitution Cipher (1/4)

- 由於加法、乘法和仿射加密法的金鑰範圍很小，所以很容易受到暴力攻擊。
- 更好的解決方法就是建立明文每個字元和其密文字元之間的對應，使得 Alice 和 Bob 能公開陳列每個字元的對應。
- 這些方法都有以下兩點特徵
 - 使用了一組相關的單字母替換規則
 - 透過金鑰來決定使用哪種特定的規則進行轉換

Monoalphabetic Substitution Cipher (2/4)

- 單字母取代加密法的金鑰範例：

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

- 我們可以使用上述的金鑰加密以下訊息

this message is easy to encrypt but hard to find the key

其密文如下

ICFVQRVVNEFVRNVSIYRGAHSLIOJICNHTIYBFGTICRXRS

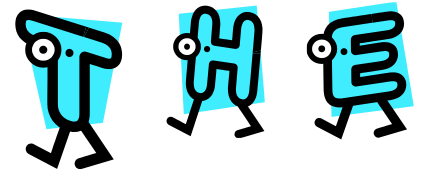
Monoalphabetic Substitution Cipher (3/4)

- Permutation
 - Of a finite set of elements S is an ordered sequence of all the elements of S , with each element appearing exactly once
- If the “cipher” line can be any permutation of the 26 alphabetic characters, then there are $26!$ or greater than 4×10^{26} possible keys
 - This is 10 orders of magnitude greater than the key space for DES
 - Approach is referred to as a *monoalphabetic substitution cipher* because a single cipher alphabet is used per message

Monoalphabetic Substitution Cipher (4/4)

- Easy to break because they reflect the frequency data of the original alphabet
- 可利用英文的雙字母組 (Bigram) 和三字母組 (Trigram) 的頻率來攻擊

雙字母組	TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
三字母組	THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH



- Countermeasure is to provide multiple substitutes (homophones) for a single letter

Polyalphabetic Ciphers

- 在多字母加密法 (Polyalphabetic Cipher) 中，每一個字元的出現都可能有不同的代換，明文裡的一個字元和密文裡的一個字元之間的關係是一對多。
- All these techniques have the following features in common:
 1. A set of related monoalphabetic substitution rules is used.
 2. A key determines which particular rule is chosen for a given transformation.

Autokey Cipher (1/2)

- 自動金鑰加密法 (Autokey Cipher) 的密鑰開頭是一個關鍵詞，之後則是明文的重複。

$$P = P_1P_2P_3\cdots \quad C = C_1C_2C_3\cdots \quad k = (k_1, P_1, P_2, \cdots)$$

$$\text{加密: } C_i = (P_i + k_i) \bmod 26 \quad \text{解密: } P_i = (C_i - k_i) \bmod 26$$

Autokey Cipher (2/2)

- 假設 Alice 和 Bob 同意使用初始金鑰值為 $k_1 = 12$ 的自動金鑰加密法。現在 Alice 要傳送訊息「Attack is today」的訊息給 Bob，密碼會一個字元一個字元地加密而成

明文：	a	t	t	a	c	k	i	s	t	o	d	a	y
P值：	00	19	19	00	02	10	08	18	19	14	03	00	24
金鑰串流：	12	00	19	19	00	02	10	08	18	19	14	03	00
C值：	12	19	12	19	02	12	18	00	11	7	17	03	24
密文：	M	T	M	T	C	M	S	A	L	H	R	D	Y

Playfair Cipher (1/3)

- Best-known multiple-letter encryption cipher
- Treats bigrams in the plaintext as single units and translates these units into ciphertext bigrams (a great advance over simple monoalphabetic ciphers since there are $26 \times 26 = 676$ bigrams)
- Based on the use of a 5×5 matrix of letters constructed using a keyword
- Invented by British scientist Sir Charles Wheatstone in 1854
- Used as the standard field system by the British Army in World War I and the U.S. Army and other Allied forces during World War II

Playfair Cipher (2/3)

- Playfair Key Matrix
 - Fill in letters of keyword (minus duplicates) from left to right and from top to bottom, then fill in the remainder of the matrix with the remaining letters in alphabetic order
 - Using the keyword 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

Playfair Cipher (3/3)

- 為了方便舉例，假設 Playfair Cipher 的密鑰如下 (其中 J 以 I 取代)

密鑰 =

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

- 我們使用下圖中的金鑰來加密明文「hello」

he → EC lx → QZ lo → BX

明文：hello 密文：ECQZBX

Vigenère Cipher (1/4)

- Best known and one of the simplest polyalphabetic substitution ciphers.
- In this scheme the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25.
- Each cipher is denoted by a key letter which is the ciphertext letter that substitutes for the plaintext letter 'a'.
- A Caesar cipher with a shift of 3 is denoted by the key value 3.

Vigenère Cipher (2/4)

- To encrypt a message, a key is needed that is as long as the message
- Usually, the key is a repeating keyword (k_1, k_2, \dots, k_m)

$$P = P_1P_2P_3\cdots \quad C = C_1C_2C_3\cdots \quad k = [(k_1, k_2, \dots, k_m), (k_1, k_2, \dots, k_m), \cdots]$$

加密： $C_i = P_i + k_i$ 解密： $P_i = C_i - k_i$

- Vigenère cipher 可視為 m 個加法加密法的組合。
- Caesar cipher 可視為 Vigenère cipher 在 $m = 1$ 時的特例。

Vigenère Cipher (3/4)

- 我們可用 6 個字母的關鍵字「PASCAL」加密訊息「She is listening」，初始金鑰流為 (15, 0, 18, 2, 0, 11)，而金鑰流為此初始金鑰串流之重複(需要幾次就重複幾次)。

明文：

P 值：

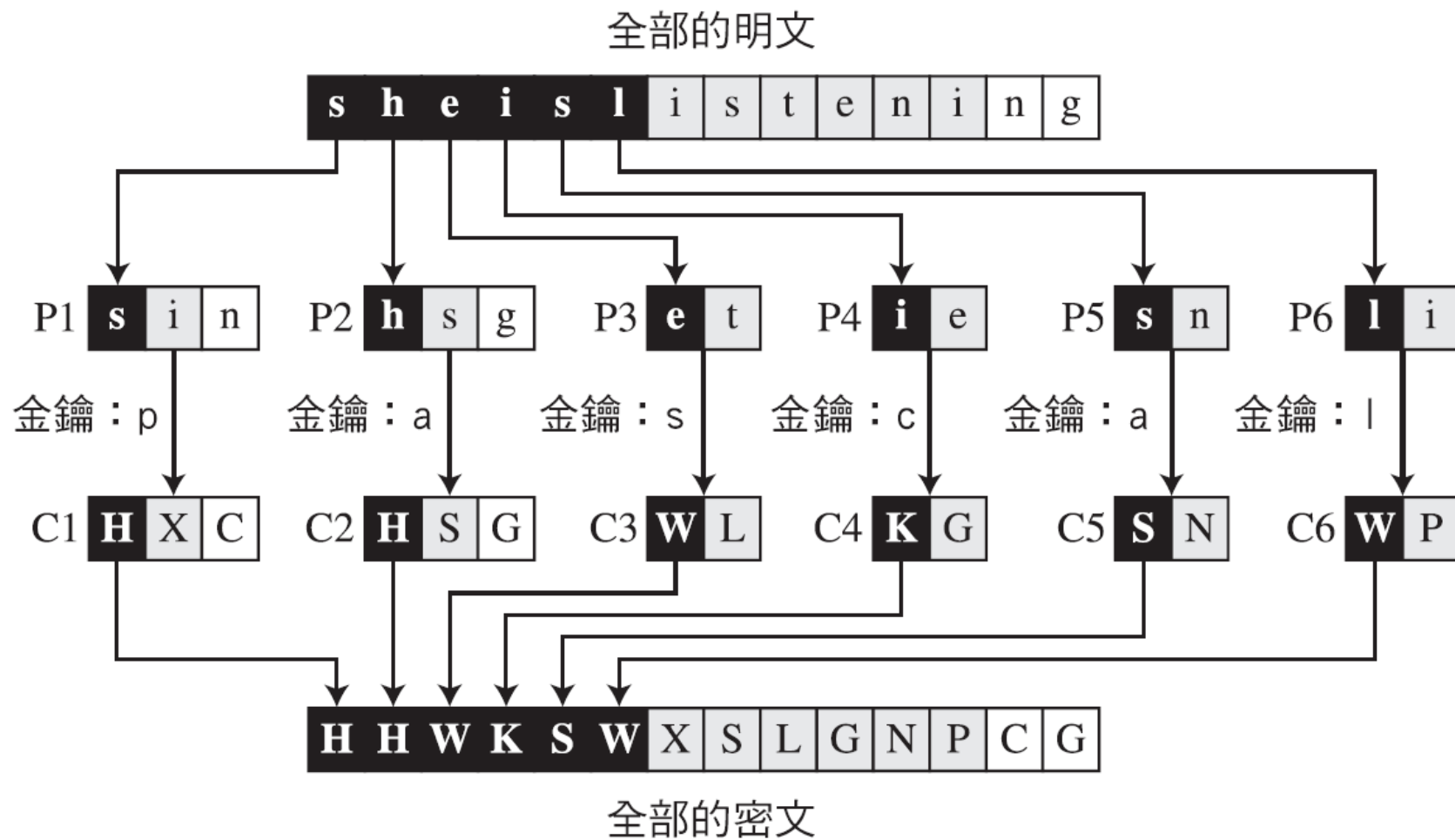
金鑰串流：

C 值：

密文：

s	h	e	i	s	l	i	s	t	e	n	i	n	g
18	07	04	08	18	11	08	18	19	04	13	08	13	06
15	00	18	02	00	11	15	00	18	02	00	11	15	00
07	07	22	10	18	22	23	18	11	6	13	19	02	06
H	H	W	K	S	W	X	S	L	G	N	T	C	G

Vigenère Cipher (4/4)



Vigenère Table

Plaintext

Key

	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	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

Plaintext: s h e ...
Key: P A S ...
Ciphertext: H H W ...

Ciphertext

Vigenère Cipher 的破密分析 (1/2)

- 假設我們截取到以下密文：

LIOMWGFEGGDVWGHHCQUCRHRWAGWIOUWLKKGZETKKMEVLWPCZVGTH-
VTSGXQOVGCSVETQLTJSUMVWVEUVLXEWSLGFZMVVWLGYHCUSWXQH-
KVGSHEEVFLCFDGVSUMPHKIRZDMPHHBVVWVWJWIXGFWLTSHGJOUEEHH-
VUCFVGOWICQLTJSUXGLW

以三個字母區段重複的Kasiski測試產生的結果

字串	第一個索引	第二個索引	差
JSU	68	168	100
SUM	69	117	48
VWV	72	132	60
MPH	119	127	8

Vigenère Cipher 的破密分析 (2/2)

- 差之最大公因數為 4，表示金鑰長度是 4 的倍數，先試 $m = 4$ ，再將密文分成四份。

```
C1: LWGWCRAOKTEPGTQCTJV  
P1: jueuapymircneroarht  
C2: IGGGQHGWGKVCTSOSQSW  
P2: ussstctsiswhofeaecei  
C3: OFDHURWQZKLZHGVVLUV  
P3: lcaerotnwhiwedssirs  
C4: MEVHCWILEMWVXGETME  
P4: iardysehaisrrtcapia
```

- 以下的部分明文是合理的：

**Julius Caesar used a cryptosystem in his war, which is now referred to as Caesar cipher.
It is a ...**

Hill Cipher (1/5)

- Developed by the mathematician Lester Hill in 1929
- Strength is that it completely **hides single-letter frequencies**
 - The use of a larger matrix hides more frequency information
 - A $m \times m$ Hill cipher hides not only single-letter but also two-letter frequency information
- Strong **against a ciphertext-only attack** but **easily broken with a known plaintext attack** (only need m plaintext-ciphertext pairs).

Hill Cipher (2/5)

- Hill 加密法的金鑰

$$\mathbf{K} = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix}$$

- Hill 加密法中的金鑰方陣需有乘法反元素。

Hill Cipher (3/5)

- 舉例來說，在明文「code is ready」最後一個區塊裡加上假字元「z」，並移除空格，會產生一個 3×4 的矩陣。其密文為「OHKNIHGKLISS」

$$\begin{matrix} & \mathbf{C} \\ \begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix} & = & \begin{matrix} & \mathbf{P} \\ \begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix} \end{matrix} & \begin{matrix} & \mathbf{K} \\ \begin{bmatrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \\ 03 & 23 & 21 & 08 \end{bmatrix} \end{matrix} \end{matrix}$$

a. 加密

$$\begin{matrix} & \mathbf{P} \\ \begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix} & = & \begin{matrix} & \mathbf{C} \\ \begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix} \end{matrix} & \begin{matrix} & \mathbf{K}^{-1} \\ \begin{bmatrix} 02 & 15 & 22 & 03 \\ 15 & 00 & 19 & 03 \\ 09 & 09 & 03 & 11 \\ 17 & 00 & 04 & 07 \end{bmatrix} \end{matrix} \end{matrix}$$

b. 解密

Hill Cipher (4/5)

- 假設 Eve 知道 $m = 3$ ，並且已攔截了三個明文／密文組合區塊（不須來自於同一個訊息）。

$$\begin{array}{ccc} \left[\begin{array}{ccc} 05 & 07 & 10 \end{array} \right] & \longleftrightarrow & \left[\begin{array}{ccc} 03 & 06 & 00 \end{array} \right] \\ \left[\begin{array}{ccc} 13 & 17 & 07 \end{array} \right] & \longleftrightarrow & \left[\begin{array}{ccc} 14 & 16 & 09 \end{array} \right] \\ \left[\begin{array}{ccc} 00 & 05 & 04 \end{array} \right] & \longleftrightarrow & \left[\begin{array}{ccc} 03 & 17 & 11 \end{array} \right] \\ \mathbf{P} & & \mathbf{C} \end{array}$$

Hill Cipher (5/5)

- 由此組合中，她求得矩陣 P 和 C ，因為 P 是可逆的，並與 C 相乘，得到 K 矩陣。

$$\begin{array}{ccc} \left[\begin{array}{ccc} 02 & 03 & 07 \\ 05 & 07 & 09 \\ 01 & 02 & 11 \end{array} \right] & = & \left[\begin{array}{ccc} 21 & 14 & 01 \\ 00 & 08 & 25 \\ 13 & 03 & 08 \end{array} \right] \left[\begin{array}{ccc} 03 & 06 & 00 \\ 14 & 16 & 09 \\ 03 & 17 & 11 \end{array} \right] \\ \mathbf{K} & & \mathbf{P}^{-1} \quad \mathbf{C} \end{array}$$

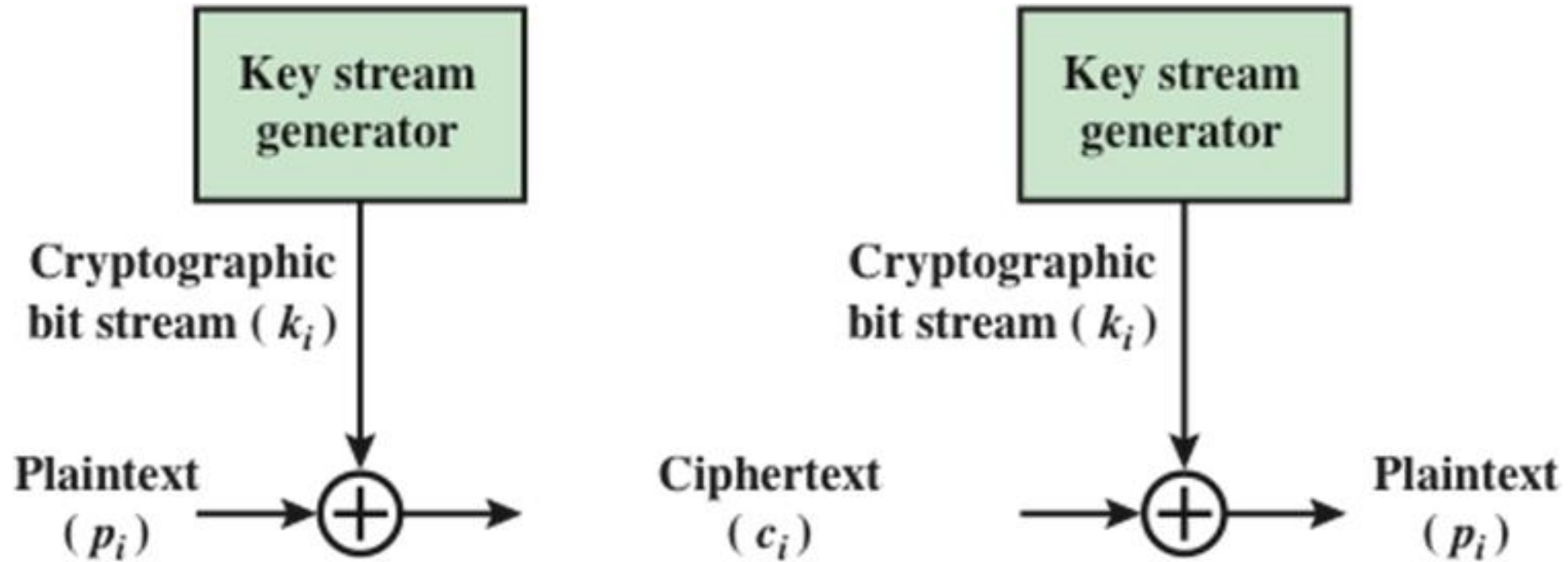
現在她有金鑰能破解任何使用此金鑰加密的密文。

One-Time Pad (1/3)

- 密碼學的目標之一就是能完全保密。Shannon 的研究表示，若每個明文的符號都由一個金鑰範圍隨機挑出的一把金鑰加密，就能達到完全保密。
- 此概念用於 **Gilbert Vernam** 在貝爾實驗室所發明的一次性密碼本（One-Time Pad，簡稱 OTP）。

One-Time Pad (2/3)

- Vernam Cipher



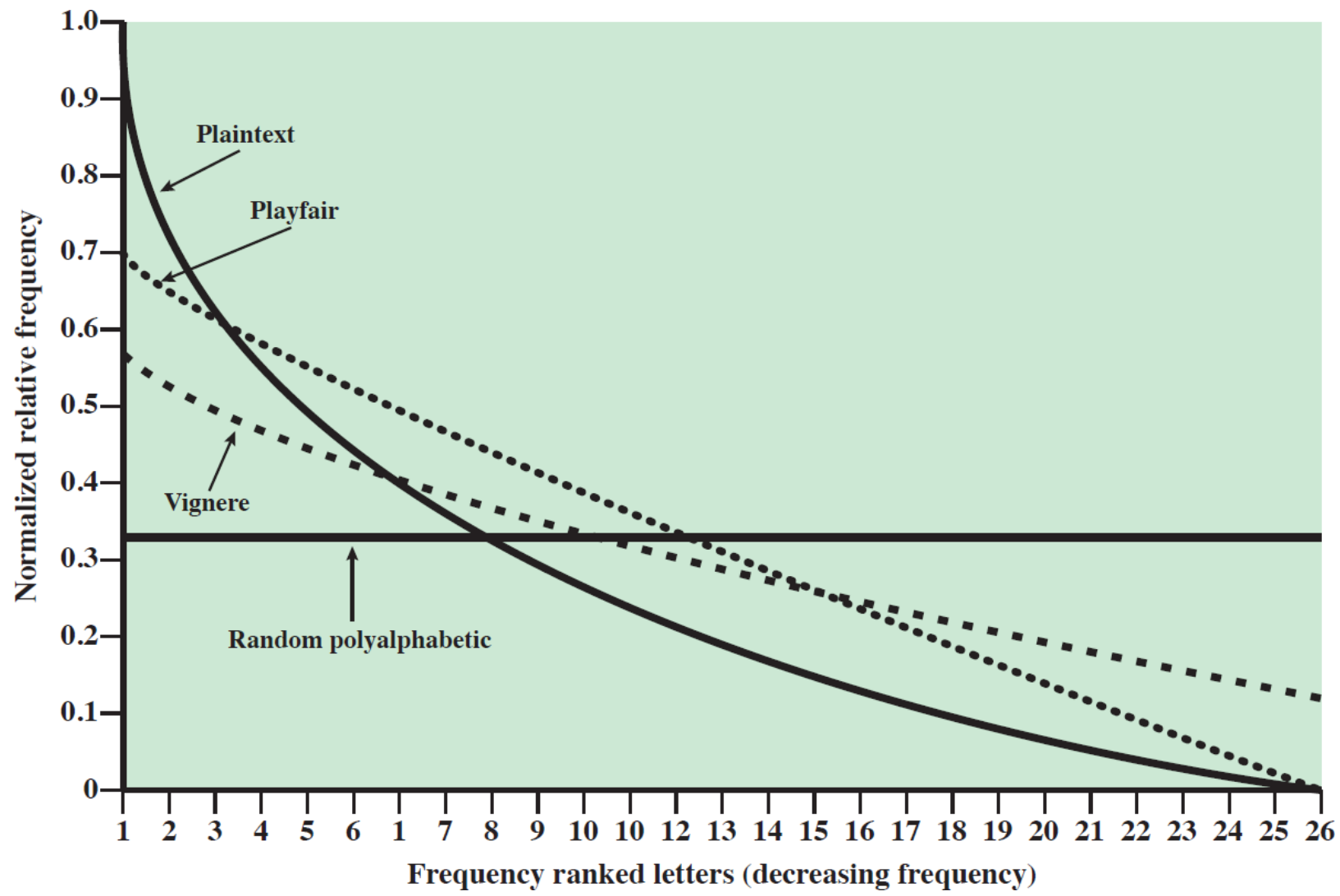
One-Time Pad (3/3)

- Improvement to Vernam cipher proposed by an Army Signal Corp officer, Joseph Mauborgne
- Use a random key that is as long as the message so that the key need not be repeated
- Key is used to encrypt and decrypt a single message and then is discarded
- Each new message requires a new key of the same length as the new message
- Scheme is unbreakable
 - Produces random output that bears no statistical relationship to the plaintext
 - Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code



Difficulties

- The **one-time pad** offers complete security but, in practice, has two fundamental difficulties:
 - There is the practical problem of making large quantities of random keys
 - Any heavily used system might require millions of random characters on a regular basis
 - Mammoth key distribution problem
 - For every message to be sent, a key of equal length is needed by both sender and receiver
- Because of these difficulties, the one-time pad is of limited utility
 - Useful primarily for low-bandwidth channels requiring very high security
- The one-time pad is the only cryptosystem that exhibits *perfect secrecy*



Relative Frequency of Occurrence of Letters

Transposition Ciphers

- 換位加密法 (Transposition Ciphers) 並不是更換符號，而是改變符號的位置。
- 有以下兩種方式
 - 無金鑰的換位加密法 (Transposition Ciphers without Key)
 - 有金鑰的換位加密法 (Transposition Ciphers with Key)

Transposition Ciphers without Key (1/4)

- 過去使用簡單的換位加密法是無金鑰的。
- 一個很好的無金鑰加密法範例就是反轉換位加密法。

明文：meet me monday morning

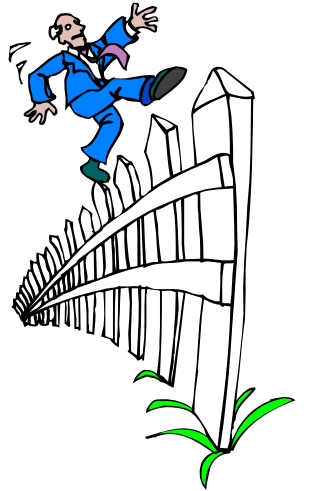
密文：GNINROM YADNOM EM TEEM

Transposition Ciphers without Key (2/4)

- 第二個無金鑰換位加密法的範例是鐵軌柵欄加密法 (Rail Fence Cipher)。在此加密法中，明文是編排成兩排 Z 字形的圖樣 (也就是一行一行的)，而密文是一列一列的圖樣。例如，Alice 傳送「meet me at the park」的訊息給 Bob。

m e m a t t e a k
 ↘ ↗ ↘ ↗ ↘ ↗ ↘ ↗ ↘ ↗
 e t e t h p r

她產生出密文「MEMATEAKETETHPR」。



Transposition Ciphers without Key (3/4)

- 第三個方法為 Alice 和 Bob 同意使用行數的換位加密法：假設 Alice 和 Bob 協議以四行為一個單位，則 Alice 會在一個四行的表格中，以一系列一列的方式寫入相同的明文。

m	e	e	t
m	e	a	t
t	h	e	p
a	r	k	

並以一行一行的方式產生出密文「**MMTAEEHREAEKTTP**」。

Transposition Ciphers without Key (4/4)

- 以下所示為第三個方法明文中的每個字元調換成密文的位置排列。

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
01	05	09	13	02	06	10	13	03	07	11	15	04	08	12

明文中的第二個字元移動至密文的第五個位置；第三個字元移動至第九個位置，以此類推。字元雖被調換，但卻是依照某個調換模式：(01, 05, 09, 13), (02, 06, 10, 13), (03, 07, 11, 15)和(08, 12)。每個區塊中，兩個鄰近號碼的差為 4。

Transposition Ciphers with Key

- 無金鑰的換位加密法調換字元是以一種方式寫入明文(如一系列一系列的)，再以另一種方式讀取(如一行一行的)，它是調換整個明文後才產生密文。
- 而有金鑰的換位加密法是將明文分組（稱為區塊），再利用一個金鑰分別更換每個區塊的字元，例如行換位加密法 (Columnar Transposition Cipher)。

Columnar Transposition Cipher (1/6)

明文：ship equipment on the fourth of july (橫列)

1	2	3	4	5		3	5	4	2	1
s	h	i	p	e		I	E	P	H	S
q	u	i	p	m		I	M	P	U	Q
e	n	t	o	n		T	N	O	N	E
t	h	e	f	o		E	O	F	H	T
u	r	t	h	o		T	O	H	R	U
f	j	u	l	y		U	Y	L	J	F

密文：IITETU EMNOOY PPOFHL HUNHRJ SQETUF (直取)

金鑰：3-5-4-2-1 (數字)

Columnar Transposition Cipher (2/6)

- Alice需要傳送「enemy attacks tonight」的訊息給Bob

e n e m y a t t a c k s t o n i g h t z

用來加密和解密的金鑰是一把排列的金鑰，顯示出字元是如何調換的。

加密 ↓

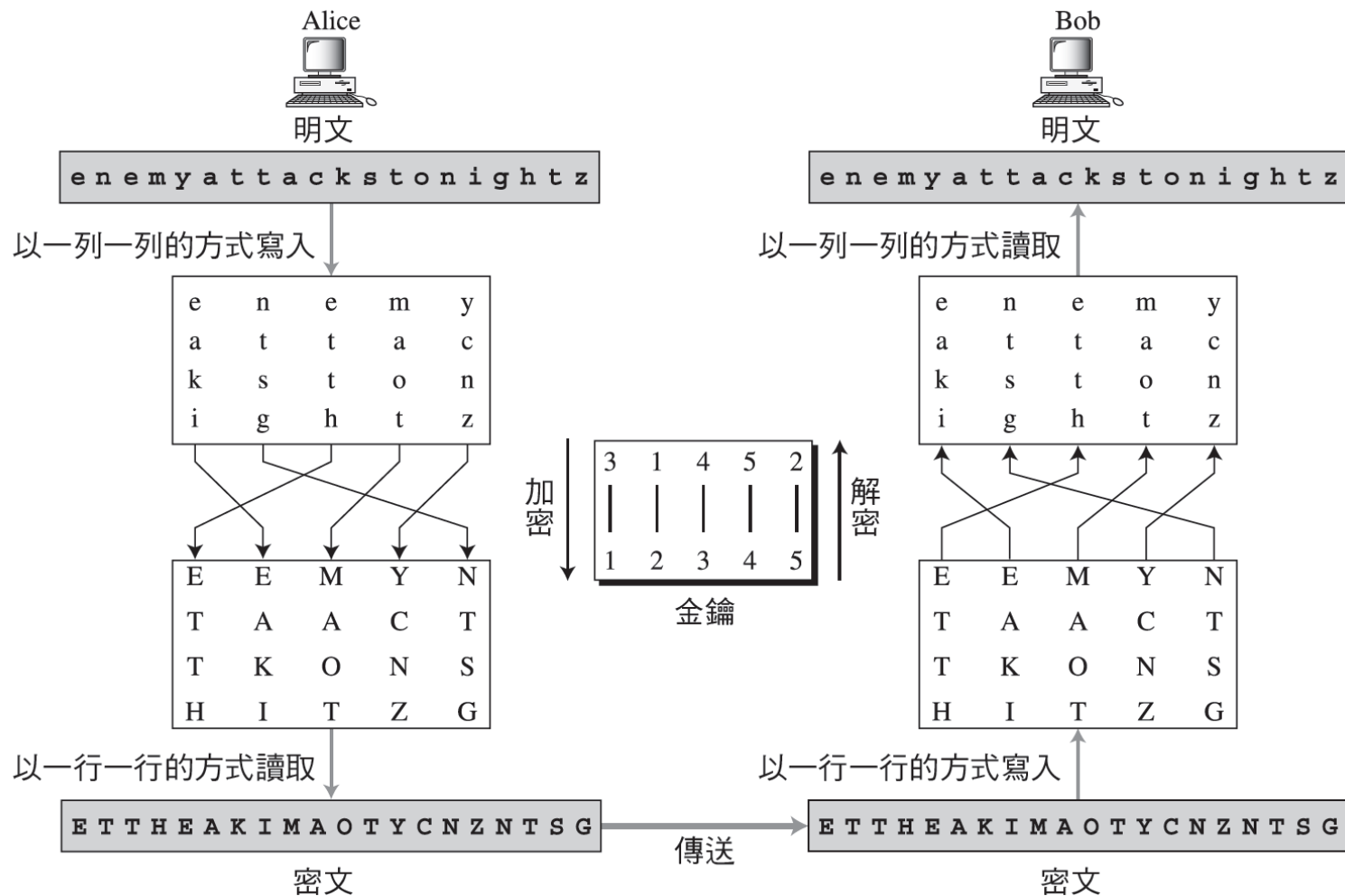
3	1	4	5	2
1	2	3	4	5

↑ 解密

經過排列產生

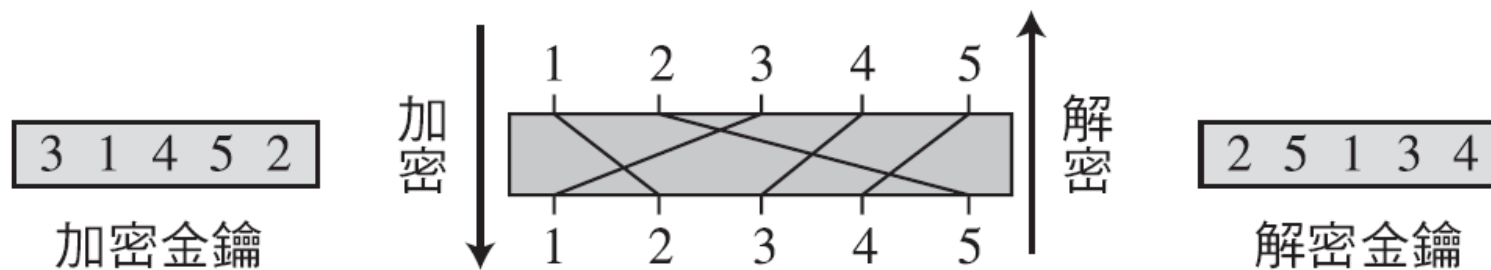
E T T H E A K I M A O T Y C N Z N T S G

Columnar Transposition Cipher (3/6)



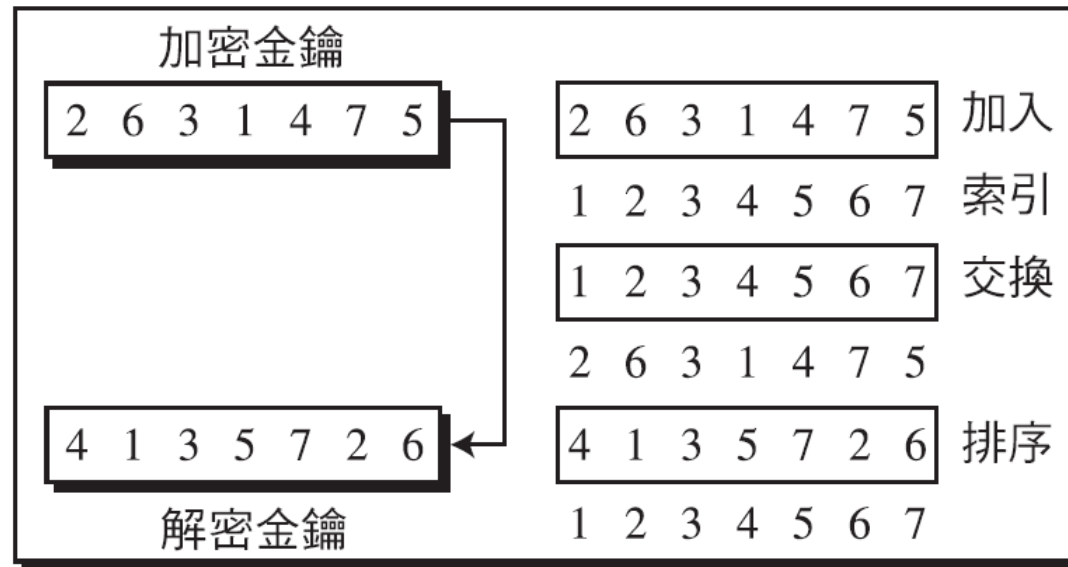
Columnar Transposition Cipher (4/6)

- 利用一個簡單的金鑰，以兩個方向做行數的調換：加密是向下，解密是向上。此圖像顯示會慣例性地產生兩個金鑰：一個為加密用，另一個用於方向。
- 换位加密法的加密／解密金鑰



Columnar Transposition Cipher (5/6)

- 换位加密法的金鑰倒轉



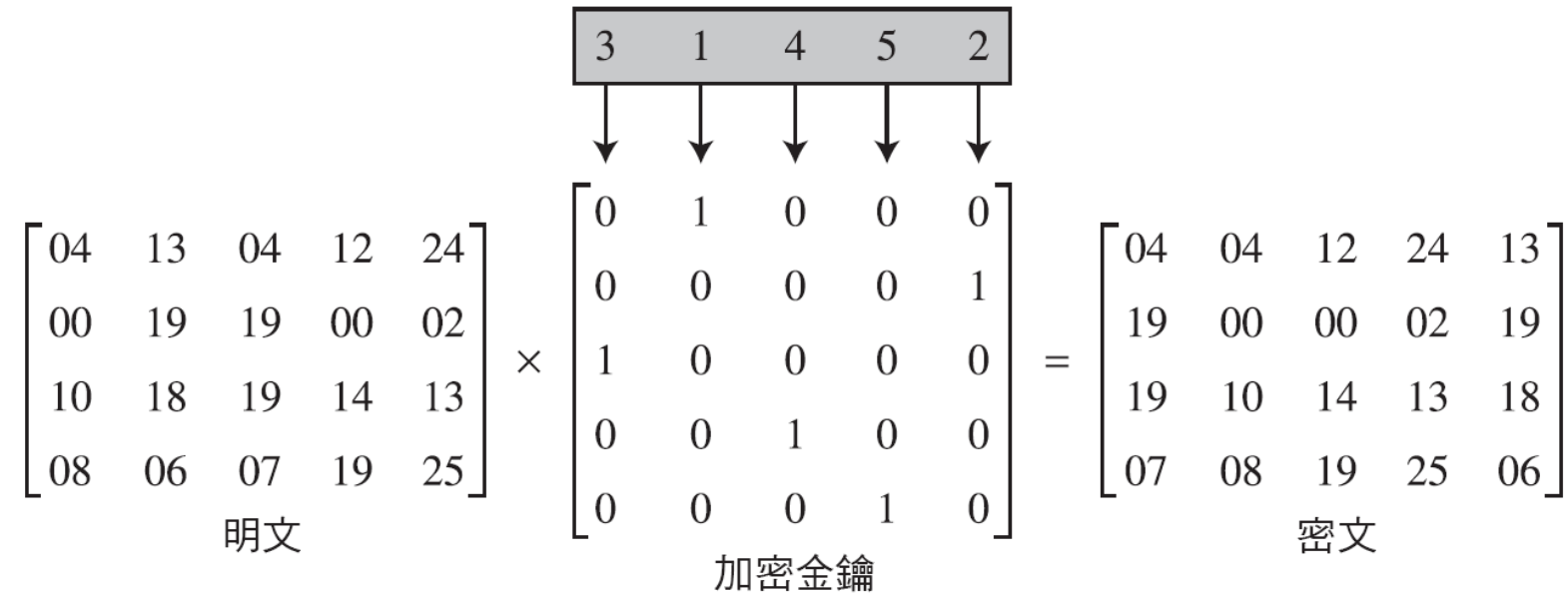
a. 流程

```
Given: EncKey [index]
index ← 1
while (index ≤ Column)
{
    DecKey[EncKey[index]] ← index
    index ← index + 1
}
Return : DecKey [index]
```

b. 演算法

Columnar Transposition Cipher (6/6)

- 我們可利用矩陣陳列換位加密法的加密／解密過程。
- 下圖顯示一個換位加密過程中金鑰矩陣的表示。4 × 5的明文矩陣與5 × 5的加密金鑰相乘，得到4 × 5的密文矩陣。



The diagram illustrates the encryption process of a Columnar Transposition Cipher. It shows a 4x5 plaintext matrix (明文) being multiplied by a 5x5 key matrix (加密金鑰) to produce a 4x5 ciphertext matrix (密文). The key matrix is derived from a key sequence [3, 1, 4, 5, 2] which determines the column order. Arrows point from the key sequence to the key matrix, indicating the column permutation.

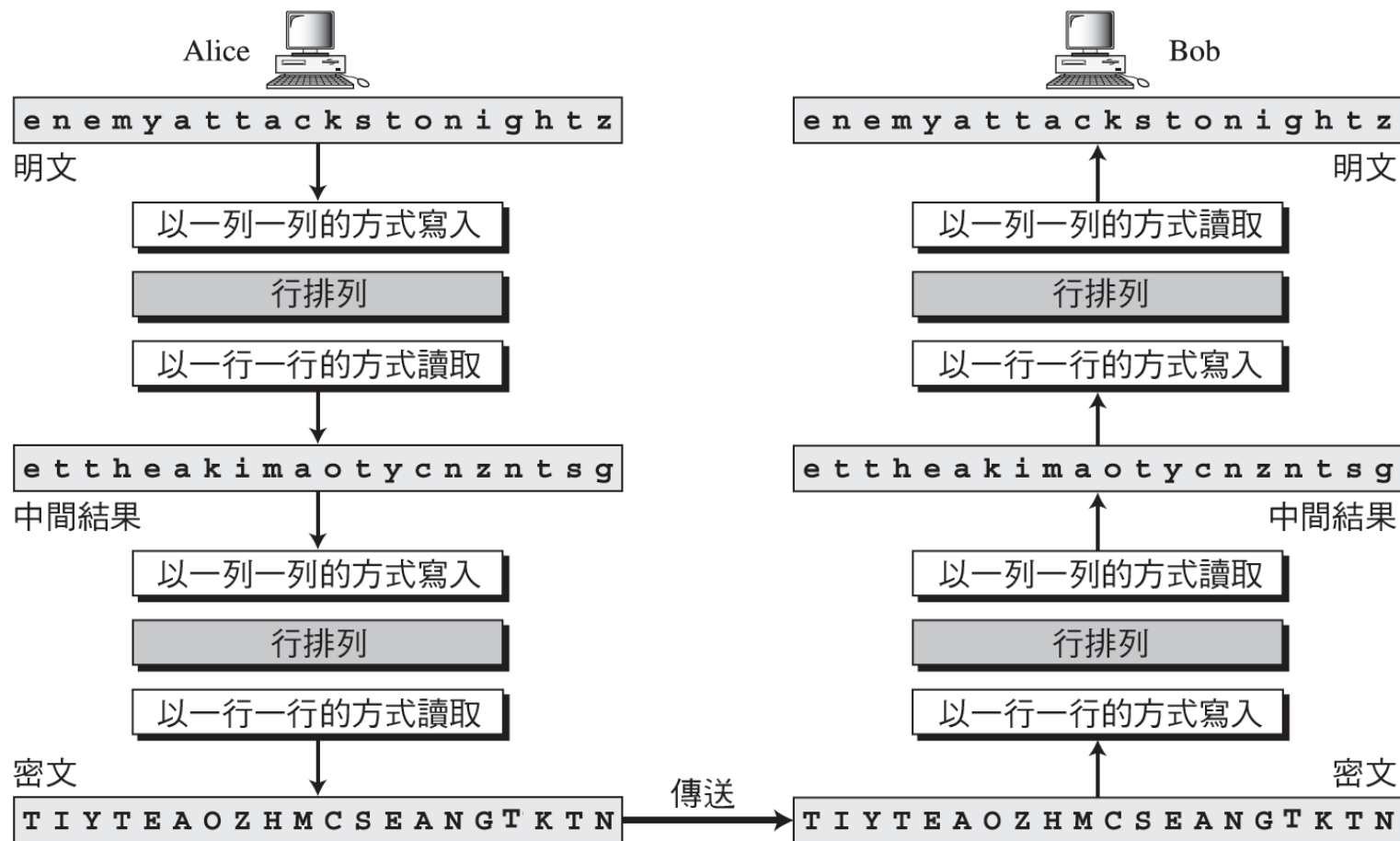
$$\begin{bmatrix} 04 & 13 & 04 & 12 & 24 \\ 00 & 19 & 19 & 00 & 02 \\ 10 & 18 & 19 & 14 & 13 \\ 08 & 06 & 07 & 19 & 25 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 04 & 04 & 12 & 24 & 13 \\ 19 & 00 & 00 & 02 & 19 \\ 19 & 10 & 14 & 13 & 18 \\ 07 & 08 & 19 & 25 & 06 \end{bmatrix}$$

明文

加密金鑰

密文

Double Transposition Cipher



Rotor Machines

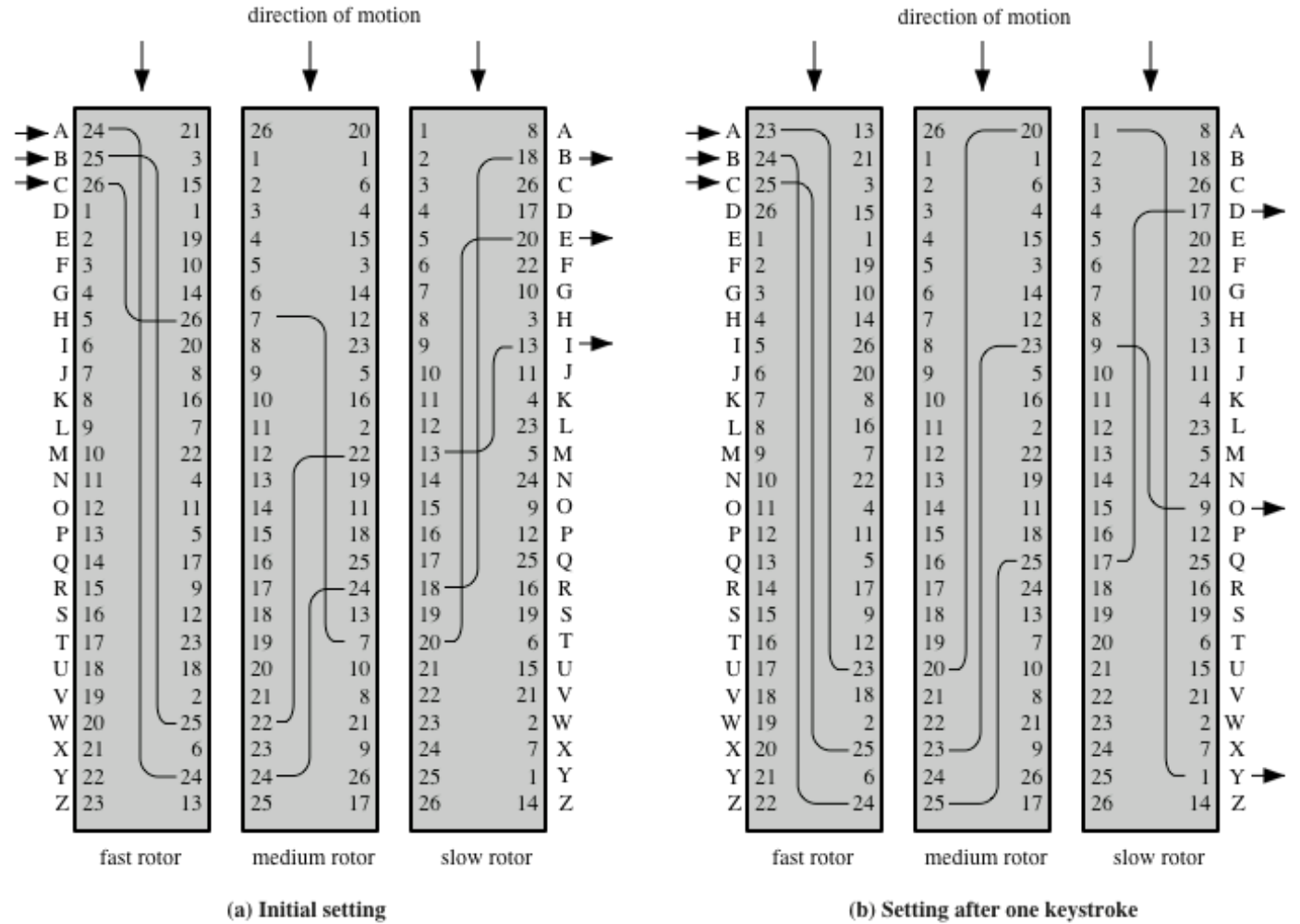
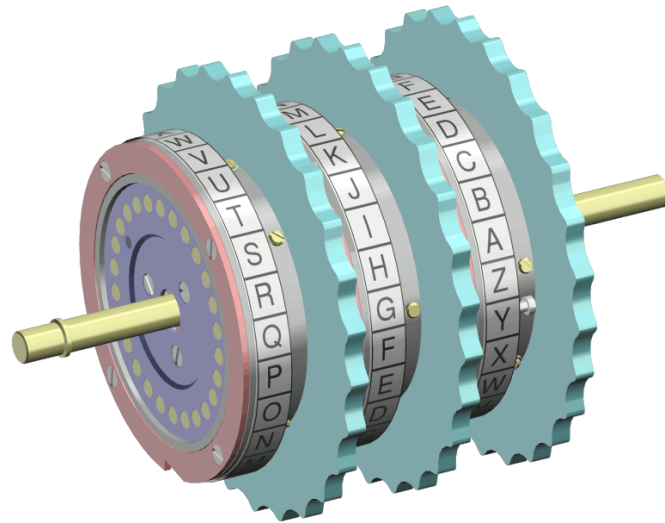


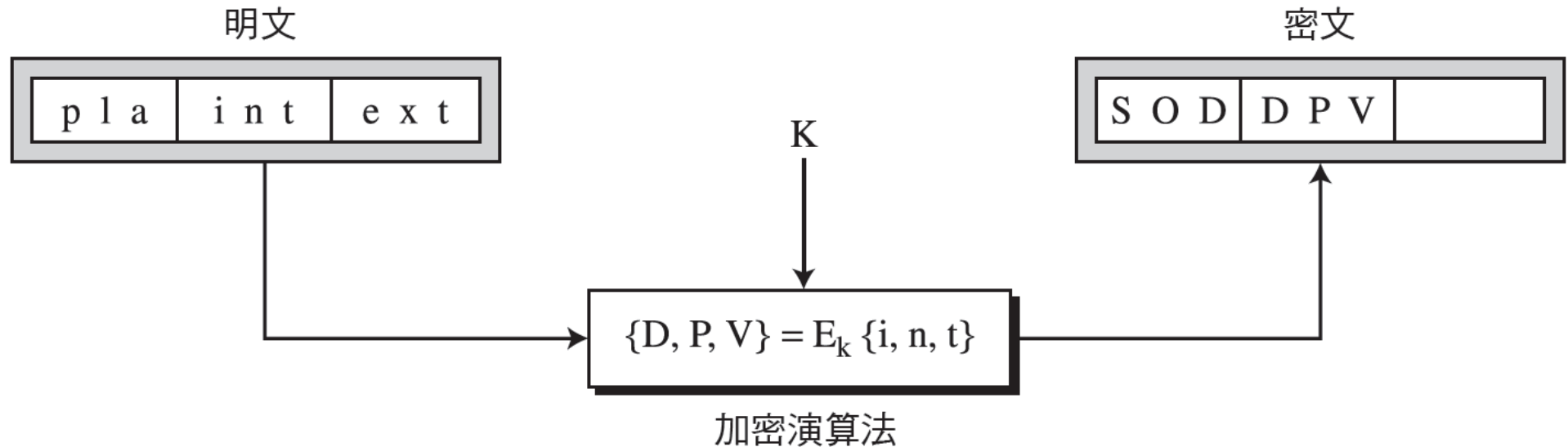
Figure 3.8 Three-Rotor Machine With Wiring Represented by Numbered Contacts

Block and Stream Ciphers

- 文獻資料將對稱式加密法分為以下兩大類：
 - Block Ciphers (區塊加密法)
 - Stream Ciphers (串流加密法)
- 雖然這種分類法被應用於現代加密法中，但這種分類法其實也可以應用於傳統加密法。

Classical Block Cipher (1/2)

- 在區塊加密法中，一組大小為 m ($m > 1$) 的明文符號會一起被加密成一組相同大小的密文。依據區塊加密法的定義，即使金鑰由多個值組成，我們只使用單一的金鑰來加密整個區塊。
- 下圖列出區塊加密法的概念：



Classical Block Cipher (2/2)

- Playfair Cipher 就是區塊加密法，其區塊大小為 $m = 2$ ，兩個字元一起被加密。
- Hill Cipher 也是區塊加密法，使用單一金鑰(矩陣)一起加密一個大小為 2 或更多的明文區塊。在此加密法中，密文每個字元的值根據所有明文字元的值而定。雖然其金鑰由 $m \times m$ 個值所組成，但還是被視為一把單一金鑰。
- 由區塊加密法的定義可明顯看出，每個區塊加密法都是多字母加密法，因為密文區塊的每個字元都根據所有明文區塊的字元而定。

Classical Stream Cipher (1/4)

- 明文串流為 P ，密文串流為 C ，而金鑰串流為 K 。

$$P = P_1P_2P_3 \cdots$$

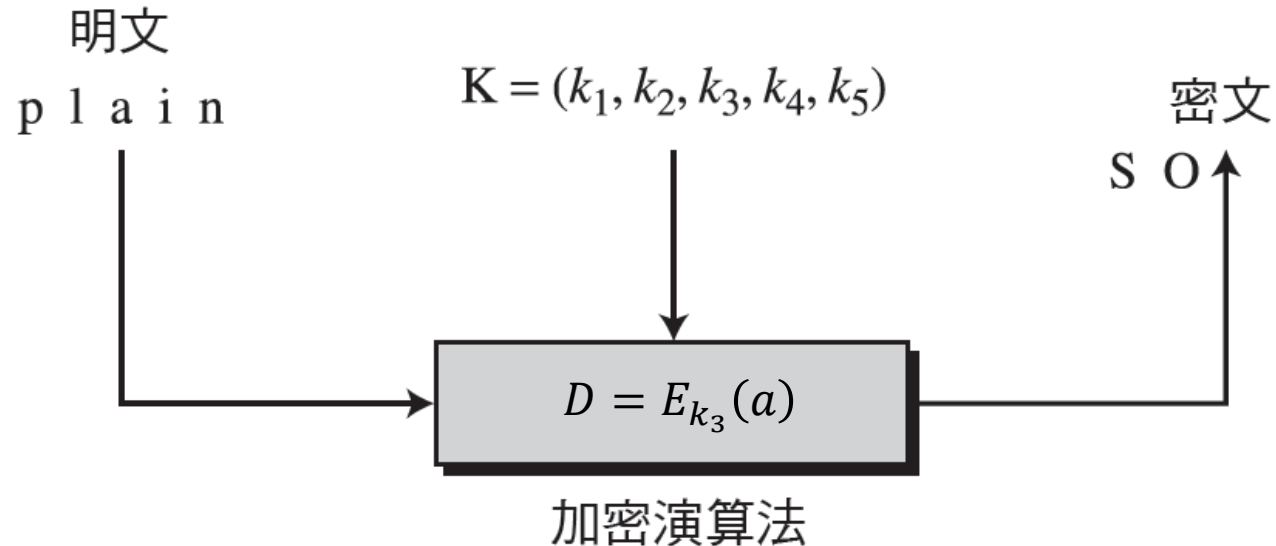
$$C = C_1C_2C_3 \cdots$$

$$K = (k_1, k_2, k_3, \cdots)$$

$$C_1 = E_{k_1}(P_1)$$

$$C_2 = E_{k_2}(P_2)$$

$$C_3 = E_{k_3}(P_3) \cdots$$



Classical Stream Cipher (2/4)

- 加法加密法可視為串流加密法的一種，因為其金鑰串流是金鑰重複的值。換句話說，金鑰串流是一個已決定好的金鑰串流或 $K = (k, k, \dots, k)$ 。無論如何，此加密法中，每個密文字元都依賴明文的對應字元，因為其金鑰流是獨立產生的。
- 本章曾討論的單字母取代加密法也屬於串流加密法。然而，每個金鑰串流的值都是明文字元在對應表的對應密文字元。
- 根據定義，Vigenère Cipher 也是串流加密法的一種。金鑰串流為重複的 m 值，其中 m 是關鍵字的大小。

$$K = (k_1, k_2, \dots, k_m, k_1, k_2, \dots, k_m, \dots)$$

Classical Stream Cipher (3/4)

- 我們能建立一個按照金鑰串流來劃分串流加密法的標準。
- 若金鑰串流中的 k_i 值並非根據明文串流中明文字元的位置而定，則此串流加密法就是單字母加密法，否則就是多字母加密法。

Classical Stream Cipher (4/4)

- 因為**加法加密法**的金鑰串流 k_i 是固定的，且並非根據明文字元的位置而定，所以加法加密法定義為單字母加密法。
- 因為**單字母取代加密法**的 k_i 並非根據明文串流中的對應字元位置而定，所以單字母取代加密法也被定義為單字母加密法。
- 因為 **Vigenère Cipher** 的 k_i 根據明文字元的位置而定，所以屬於多字母加密法。然而，其相依性是循環的，意即兩個相隔距離為 m 的字元，其加密金鑰是相同的。

The Combination

- 實際上，明文區塊是獨立加密的，但它是利用一個金鑰串流，以區塊的方式加密整個訊息。換言之，以獨立區塊來看，此加密法為**區塊加密法**；但就整個訊息而言，若將一個區塊視為一個單位，則此加密法就是**串流加密法**。
- 每個區塊使用不同的金鑰，其金鑰就有可能於加密過程前或加密過程進行時產生。