Classical Encryption Techniques

Pei-Ju (Julian) Lee

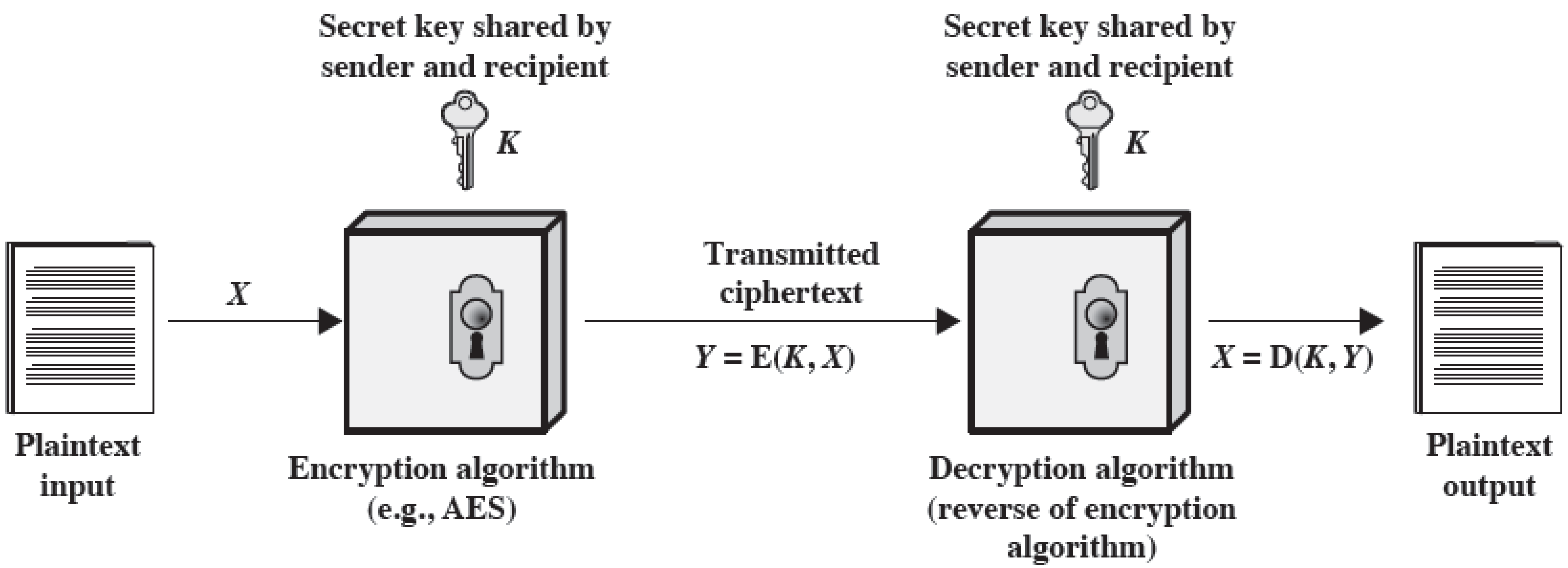
National Chung Cheng University
Information Security
pjlee@mis.ccu.edu.tw

Fall, 2016

Symmetric Encryption

- Also referred to as conventional encryption or single-key encryption
- In use prior to the development of public key encryption in the 1970s.

Simplified Model of Symmetric Encryption



- Plaintext (The original message)
- Ciphertext (The coded message)
- Enciphering or encryption (Process of converting from plaintext to ciphertext)
- Deciphering or decryption (Restoring the plaintext from the ciphertext)
- Cryptography (Study of encryption)
- Cryptographic system or cipher (Schemes used for encryption)
- Cryptanalysis (Techniques used for deciphering a message without any knowledge of the enciphering details)
- Cryptology (Areas of cryptography and cryptanalysis together)

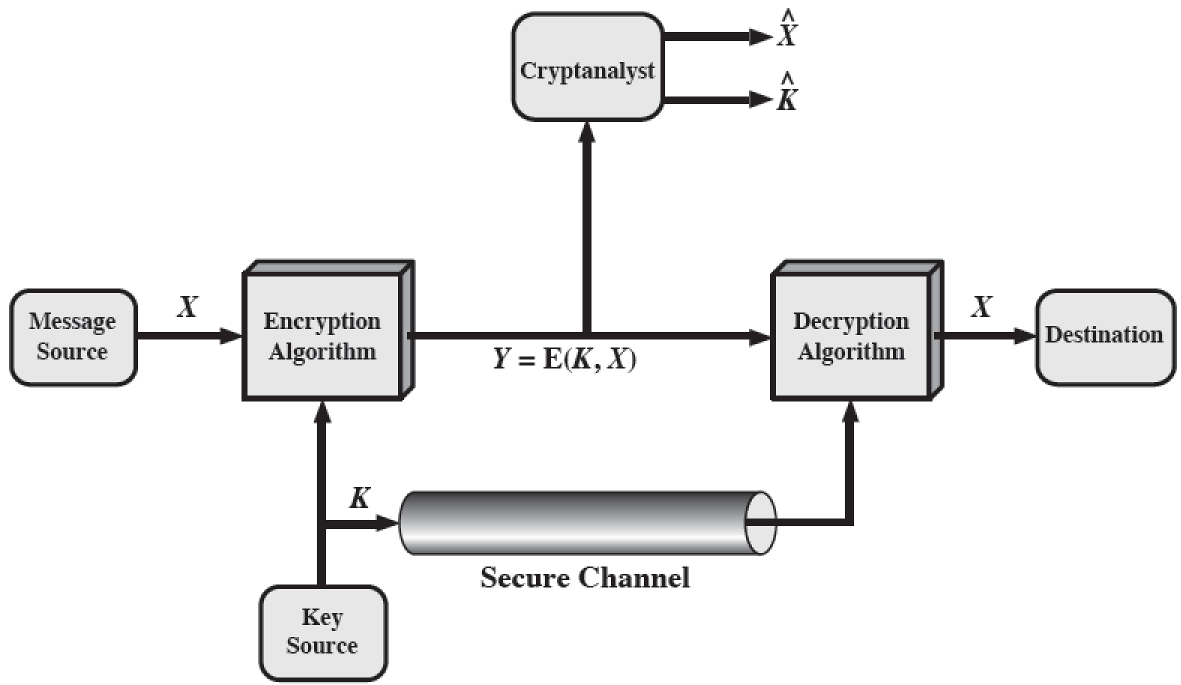
Secure Use of Conventional Encryption

- Two Requirements
  - Need a strong encryption algorithm, at a minimum, the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key.
    - A stronger form: the opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertext together with the plaintext that produced each ciphertext.
  - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

Model of Symmetric Cryptosystem

- Don't need to keep the algorithm secret; but only keep the key secret
  - Low-cost chip implementation of data encryption algorithms

- Plaintext: $X=[X_1,\ldots X_M]$, letter, binary code
- Key: $K=[K_1, \ldots K_j]$
- Ciphertext: $Y=[Y_1,\ldots Y_N]$
- $Y=E(K,X)$: Y is produced by using encryption algorithm E as a function of the plaintext X, with the specific function determined by the value of the key K
- $X=D(K,Y)$
- Plaintext estimate: $\hat{X}$
- Key estimate: $\widehat{K}$



Cryptographic Systems

- Characterized along three independent dimensions:

The type of operations used for transforming plaintext to ciphertext

- Substitution
- Transposition

The number of keys used

- Symmetric, single-key, secret-key, conventional encryption
- Asymmetric, two-key, or public-key encryption

The way in which the plaintext is processed

- Block cipher
- Stream cipher

Cont’d

- Substitution:
  - each element in the plaintext (bit, letter, group of bits or letters) is *mapped* into another ciphertext element
- Transposition:
  - elements in the plaintext are *rearranged*.

Attacking approach

- Two approaches to attacking a conventional encryption scheme:

Cryptanalysis

- **Attack relies on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext**
- **Attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used**

E.g. Frequency of Occurrence of Letters

Brute-force attack

- **Attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained**
- **On average, half of all possible keys must be tried to achieve success**

E.g. Caesar cipher: Try all 25 possible keys

Type of Cryptanalytic Attacks

- Based on the amount of info. known to the cryptanalyst:
- The most difficult problem: known ciphertext only
- Easiest to defend: ciphertext only attack (least amt. of info.)

Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Encryption Scheme Security

- Two definitions of encryption scheme:
- Unconditionally secure
  - No matter how much time an opponent has, it is impossible for him or her to decrypt the ciphertext simply because the required information is not there
    - With the exception of a scheme known as the one-time pad, there is no encryption algorithm that is unconditionally secure
- Computationally secure (either one is met)
  - The cost of breaking the cipher exceeds the value of the encrypted information
  - The time required to break the cipher exceeds the useful lifetime of the information

Brute-Force Attack

Involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained

On average, half of all possible keys must be tried to achieve success

To supplement the brute-force approach, some degree of knowledge about the expected plaintext is needed, and some means of automatically distinguishing plaintext from garble is also needed

Substitution Technique

- Symmetric Encryption = classical encryption
- Techniques: substitution, transposition
  - Caesar Cipher
  - Monoalphabetic Cipher
  - Playfair Cipher
  - Hill Cipher
  - One-Time Pad

Caesar Cipher

- Can define transformation as:

  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

  – replacing each letter of the alphabet with the letter standing three places further down the alphabet

- Alphabet is wrapped around so that the letter following Z is A

plain: meet me after the toga party

cipher: PHHW PH DIWHU WKH WRJD SDUWB

Numerical Equivalent

- Mathematically give each letter a number

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

- Algorithm can be expressed as:

$$C = \mathrm{E}(3, p) = (p + 3) \bmod (26)$$

for each ciphertext letter p, substitute the ciphertext letter c.

- The general Caesar algorithm is:

$$C = E(k , p) = (p + k) \bmod 26$$

- The decryption algorithm is:

$$p = D(k , C) = (C - k) \bmod 26$$

Brute-Force Cryptanalysis of Caesar Cipher

- If known that C is a Caesar cipher
  - Try all 25 possible keys (Brute-Force)
    - 1.The encryption and decryption algorithms are known
    - 2. There are only 25 keys to try
    - 3.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 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

Sample of Compressed Text

- In most networking situations, we can assume that the algorithms are known
- Brute-force is impractical when:
  - Large number of keys (Ex. The 3DES algorithm with a 168-bit key, then the possible keys is 2^{168} or ~$3.7 * 10^{50}$)

    Computation time is too long
  - The language of the *p* is unknown

    Expected plaintext is needed

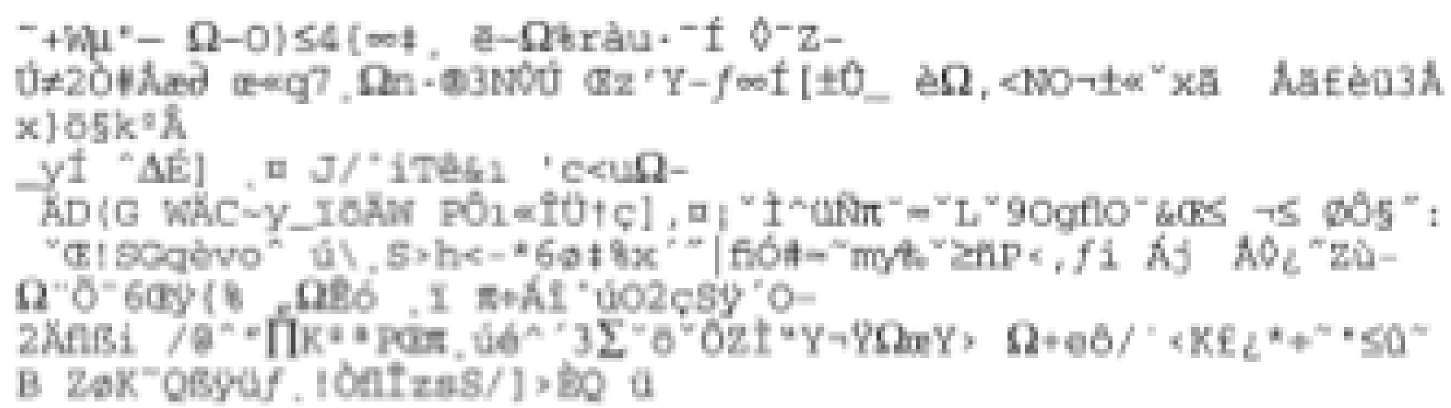


Figure 2.4 Sample of Compressed Text

Monoalphabetic Cipher

- Permutation
  - Of a finite set of elements *S* is an ordered sequence of all the elements of *S* , with each element appearing exactly once
    - Ex. S = {a, b, c}, the permutations of S : abc, acb, bac, bca, cab, cba (3! = 3*2 = 6)
- If the “cipher” line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than 4 x 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 con’d

- Ex. The ciphertext to be solved:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ

VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

Monoalphabetic con’d

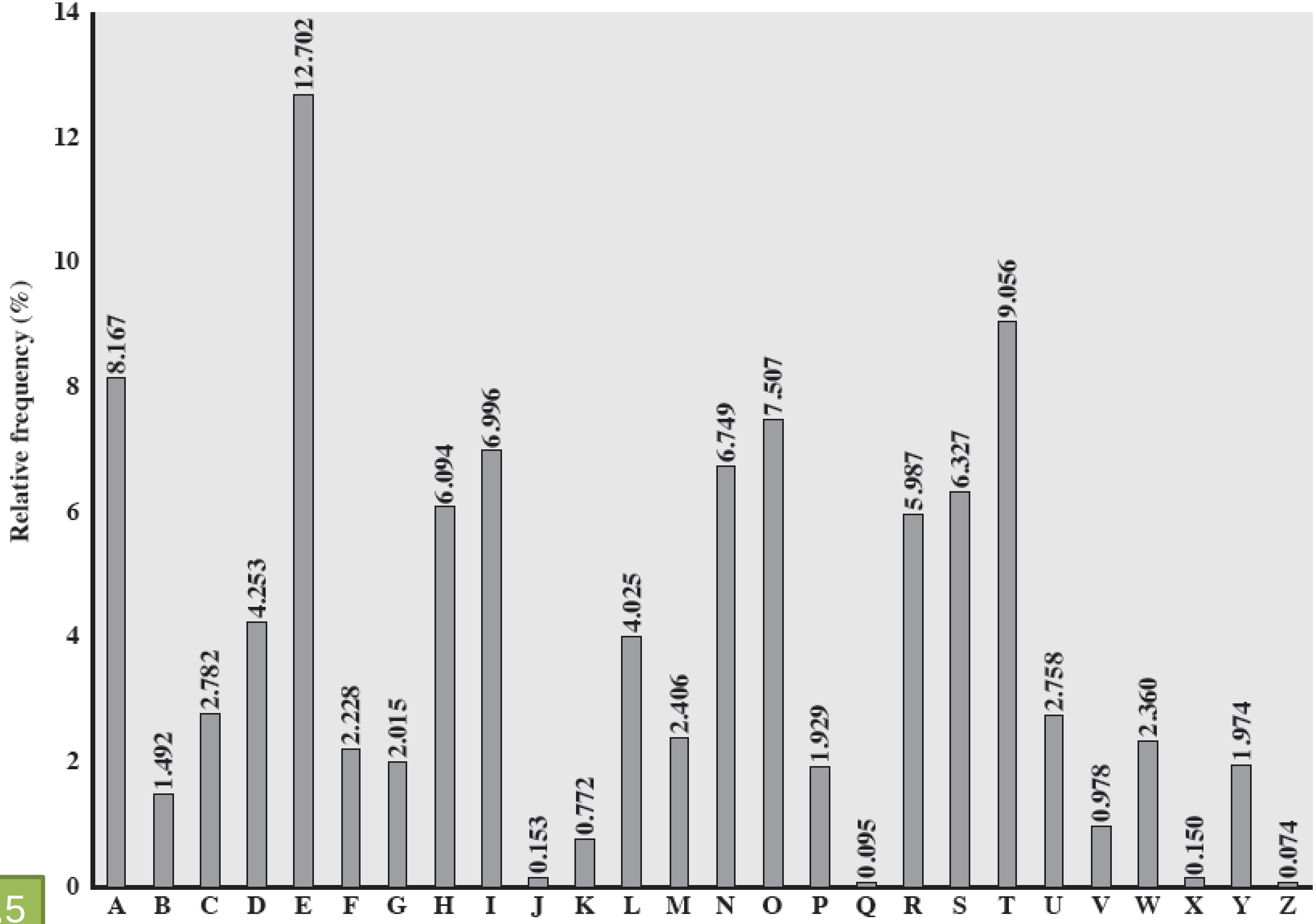
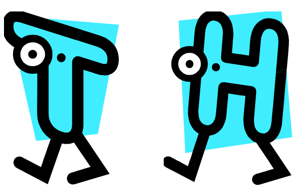


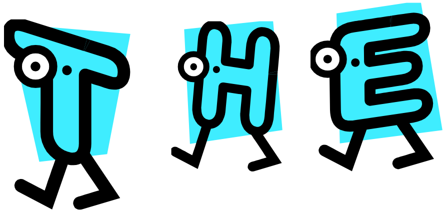
Fig 2.5

Monoalphabetic con'd

- Easy to break because they reflect the frequency data of the original alphabet
- Countermeasure is to provide multiple substitutes (homophones) for a single letter
- Digram
  - Two-letter combination
  - Most common is *th*



- Trigram
  - Three-letter combination
  - Most frequent is *the*



Monoalphabetic con'd

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

- The most common digram is th
- In ciphertext, the most common diagram is ZW

```
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
```

Methods to Disconnect P/C

- Two principal methods are used in substitution ciphers to lessen the extent to which the structure of the plaintext survives in the ciphertext:
  - to encrypt multiple letters of plaintext
  - to use multiple cipher alphabets

Playfair Cipher

- Best-known multiple-letter encryption cipher
- Treats digrams in the plaintext as single units and translates these units into ciphertext digrams
- Based on the use of a 5 x 5 matrix of letters constructed using a keyword
- Ex. 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 Key Matrix

- 1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.
- 2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.
- 3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.
- 4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

Advantages of Playfair Cipher

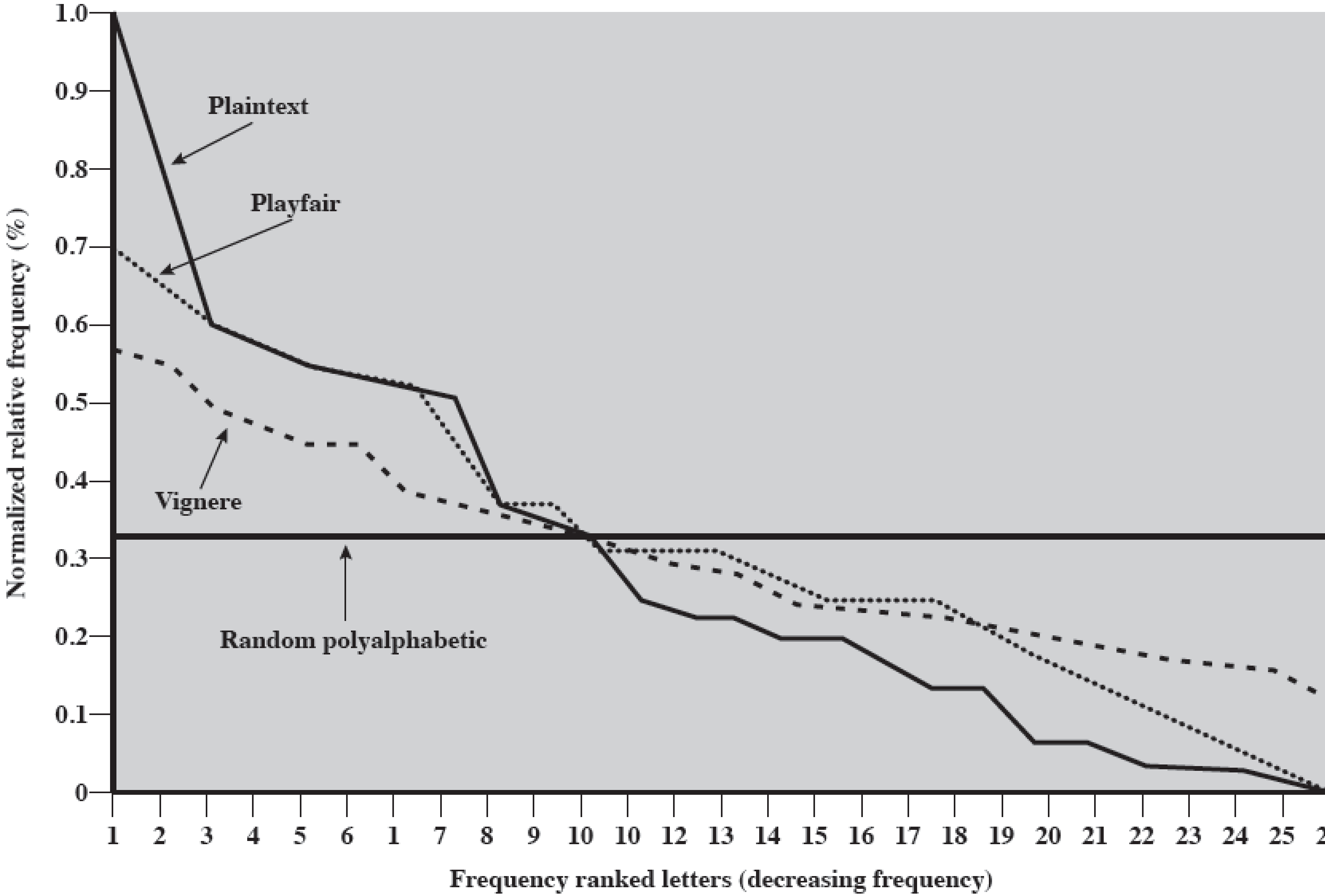
- Whereas there are only 26 letters, there are 26 * 26 = 676 digrams
  - Identification of individual digram is difficult
- The relative frequencies of individual letters exhibit a much greater range than that of digrams
- But - It is relatively easy to break
  - still leaves much of the structure of the plaintext language intact

- 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

Cont'd

- One way to check the effectiveness of the Playfair and other ciphers:
  - Analyze the Frequency of Occurrence of Letters

Relative Frequency of Occurrence of Letters



Hill Cipher

- Strength is that it completely hides single-letter frequencies
  - The use of a larger matrix hides more frequency information
  - A 3 x 3 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

Concepts from Linear Algebra

- We define the inverse $\mathbf{A}^{-1}$ of a square matrix $\mathbf{A}$ by the equation $\mathbf{A}(\mathbf{A}^{-1}) = \mathbf{A}^{-1}\mathbf{A} = \mathbf{I}$
- **I**: Identity matrix, e.g. $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$
- $\mathbf{A}^{-1}$: Inverse matrix of $\mathbf{A}$
- Example: $\mathsf{A} \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad \mathsf{A}^{-1} = \frac{1}{|\mathsf{A}|} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{a\,d - b\,c} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$
- $|\mathbf{A}|$: Determinant

Cont'd

- Example: compute $\mathbf{A}^{-1}$mod26 of known **A**

$$\mathbf{A} = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$$

$$\mathbf{A}^{-1} \bmod 26 = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$$

$$\begin{aligned} \mathbf{AA}^{-1} &= \begin{pmatrix} (5 \times 9) + (8 \times 1) & (5 \times 2) + (8 \times 15) \\ (17 \times 9) + (3 \times 1) & (17 \times 2) + (3 \times 15) \end{pmatrix} \\ &= \begin{pmatrix} 53 & 130 \\ 156 & 79 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

- −b mod N

= (−1·b) mod N

= (−1 mod N) (b mod N) mod N

= (N−1) b mod N

Cont'd

$$\mathsf{A} \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \qquad \mathsf{A}^{-1} = \frac{1}{|\mathsf{A}|}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{a\,d - b\,c}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

$$\mathsf{A} \equiv \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}, \qquad \mathsf{A}^{-1} = \frac{1}{|\mathsf{A}|}\begin{bmatrix} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} & \begin{vmatrix} a_{13} & a_{12} \\ a_{33} & a_{32} \end{vmatrix} & \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} \\ \begin{vmatrix} a_{23} & a_{21} \\ a_{33} & a_{31} \end{vmatrix} & \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} & \begin{vmatrix} a_{13} & a_{11} \\ a_{23} & a_{21} \end{vmatrix} \\ \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix} & \begin{vmatrix} a_{12} & a_{11} \\ a_{32} & a_{31} \end{vmatrix} & \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \end{bmatrix}.$$

The Hill Algorithm

For example, consider the plaintext "paymoremoney" and use the encryption key

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

The first three letters of the plaintext are represented by the vector (15 0 24). Then $(15\ 0\ 24)\mathbf{K} = (303\ 303\ 531) \bmod 26 = (17\ 17\ 11) = \text{RRL}$. Continuing in this fashion, the ciphertext for the entire plaintext is RRLMWBKASPDH.

In general terms, the Hill system can be expressed as

$$\mathbf{C} = \mathrm{E}(\mathbf{K}, \mathbf{P}) = \mathbf{PK} \bmod 26$$
$$\mathbf{P} = \mathrm{D}(\mathbf{K}, \mathbf{C}) = \mathbf{CK}^{-1} \bmod 26 = \mathbf{PKK}^{-1} = \mathbf{P}$$

Cont'd

- Although the Hill cipher is strong against a ciphertext-only attack, it is easily broken with a known plaintext attack.

$$\mathbf{C} = \mathbf{PK} \bmod 26$$

$$\mathbf{P} = \mathbf{K}^{-1}\mathbf{C} \bmod 26$$

$$\mathbf{K} = \mathbf{P}^{-1}\mathbf{C} \bmod 26$$

Example

Consider this example. Suppose that the plaintext "hillcipher" is encrypted using a 2×2 Hill cipher to yield the ciphertext HCRZSSXNSP. Thus, we know that $(7\ 8)\mathbf{K} \bmod 26 = (7\ 2)$; $(11\ 11)\mathbf{K} \bmod 26 = (17\ 25)$; and so on. Using the first two plaintext–ciphertext pairs, we have

$$\begin{pmatrix} 7 & 2 \\ 17 & 25 \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \mathbf{K} \bmod 26$$

The inverse of $\mathbf{X}$ can be computed:

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}^{-1} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}$$

so

$$\mathbf{K} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 7 & 2 \\ 17 & 25 \end{pmatrix} = \begin{pmatrix} 549 & 600 \\ 398 & 577 \end{pmatrix} \bmod 26 = \begin{pmatrix} 3 & 2 \\ 8 & 5 \end{pmatrix}$$

This result is verified by testing the remaining plaintext–ciphertext pairs.

Polyalphabetic Ciphers

- Polyalphabetic substitution cipher
  - Improves on the simple monoalphabetic technique by using different monoalphabetic substitutions as one proceeds through the plaintext message

All these techniques have the following features in common:

- A set of related monoalphabetic substitution rules is used
- A key determines which particular rule is chosen for a given transformation

Vigenère Cipher

- Best known polyalphabetic substitution ciphers
- 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
- Thus, a Caesar cipher with a shift of 3 is denoted by the key value 3

Example of Vigenère Cipher

- To encrypt a message, a key is needed that is as long as the message
- Usually, the key is a repeating keyword
- For example, if the keyword is ***deceptive***, the message "***we are discovered save yourself***" is encrypted as:

key: deceptivedeceptivedeceptive

plaintext: wearediscoveredsaveyourself

ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

a(i.e. 0)+k(i.e. 3) = d(i.e. 3)
C = (P+K)mod26 = (22+3)mod26 = 25(i.e. Z)

Example cont'd

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

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

- The strength of this cipher is that there are multiple ciphertext letters for each plaintext letter

Cryptanalysis

- Ex: the opponent believes that the *C* was encrypted using:
  - Monoalphabetic substitution
  - or a Vigenere cipher

- Test to make a determination:
  - If a monoalphabetic substitution is used:
    - Found the statistical properties of the *C* should be the same or close to the *P* as shown in Fig 2.5.
  - If a Vigenere cipher is used:
    - Found identical C sequence for two identical sequence of P letters

Vigenère Autokey System

- A keyword is concatenated with the plaintext itself to provide a running key
- Example:

  key: deceptivewearediscoveredsav

  plaintext: wearediscoveredsaveyourself

  ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA
- However,
  - Even this scheme is vulnerable to cryptanalysis
  - Because the key and the plaintext share the same frequency distribution of letters, a statistical technique can be applied

Cont’d

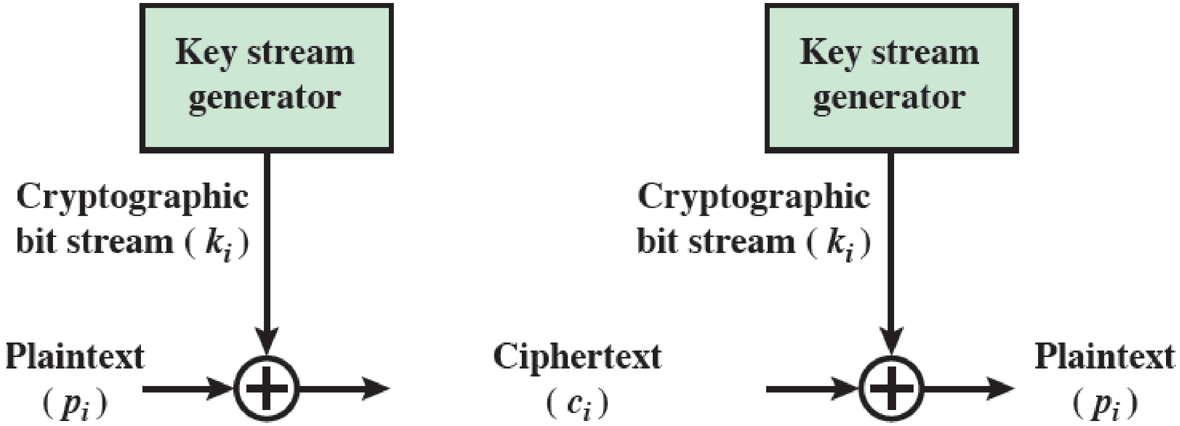
- The ultimate defense against such a cryptanalysis is:
  - to choose a keyword that is as long as the plaintext and has no statistical relationship to it.
  - Vernam Cipher: this system was introduced by an AT&T engineer named Gilbert Vernam in 1918.

Vernam Cipher

p_i = ith binary digit of plaintext
k_i = ith binary digit of key
c_i = ith binary digit of ciphertext
$\oplus$ = exclusive-or (XOR) operation

$$c_i = p_i \oplus k_i$$

$$p_i = c_i \oplus k_i$$



- Vernam cipher works on binary data (bits)
- The essence of this technique is the means of construction of the **key**

Cont'd

- However,
  - The use of a running loop of tape that eventually repeated the key
  - This scheme presents cryptanalytic difficulties, but can be broken with sufficient ciphertext, the use of known or probable plaintext sequences, or both.
- An improvement: One-Time Pad

One-Time Pad

- 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

Example

- Same *C*, different *K*:

ciphertext:	ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:	*pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih*
plaintext:	mr mustard with the candlestick in the hall

ciphertext:	ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:	*mfugpmiydgaxgoufhklllmhsqdqogtewbqfgyovuhwt*
plaintext:	miss scarlet with the knife in the library

No way to decide which key is correct and therefore which P is correct

- Difficulties:
  - Making large quantities of random keys
  - Mammoth key distribution problem
- It is of limited utility but useful primarily for low-bandwidth channels requiring very high security
- The only cryptosystem that exhibits *perfect secrecy (due to the randomness of the key)*

Transposition Techniques

- Substitution: the substitution of a ciphertext symbol for a plaintext symbol.
- Transposition: permutation of the plaintext letters
  - Rail Fence Cipher
  - Row Transposition Cipher

Rail Fence Cipher

- Rail Fence Cipher:
  - Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows
  - The message "meet me after the toga party" with a rail fence of depth 2, we would write:

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

e t e f e t e o a a t

Encrypted message is:

MEMATRHTGPRYETEFETEOAAT

Row Transposition Cipher

- Write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns
  - The order of the columns then becomes the key to the algorithm

```
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
```

Multiple Transposition

- A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext.
  - The cryptanalyst can play around with column position, or use digram or trigram frequency table
- More than one stage of transposition:

Example

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

Transposition again

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

NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

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	26	27	28

03	10	17	24	04	11	18	25	02	09	16	23	01	08
15	22	05	12	19	26	06	13	20	27	07	14	21	28

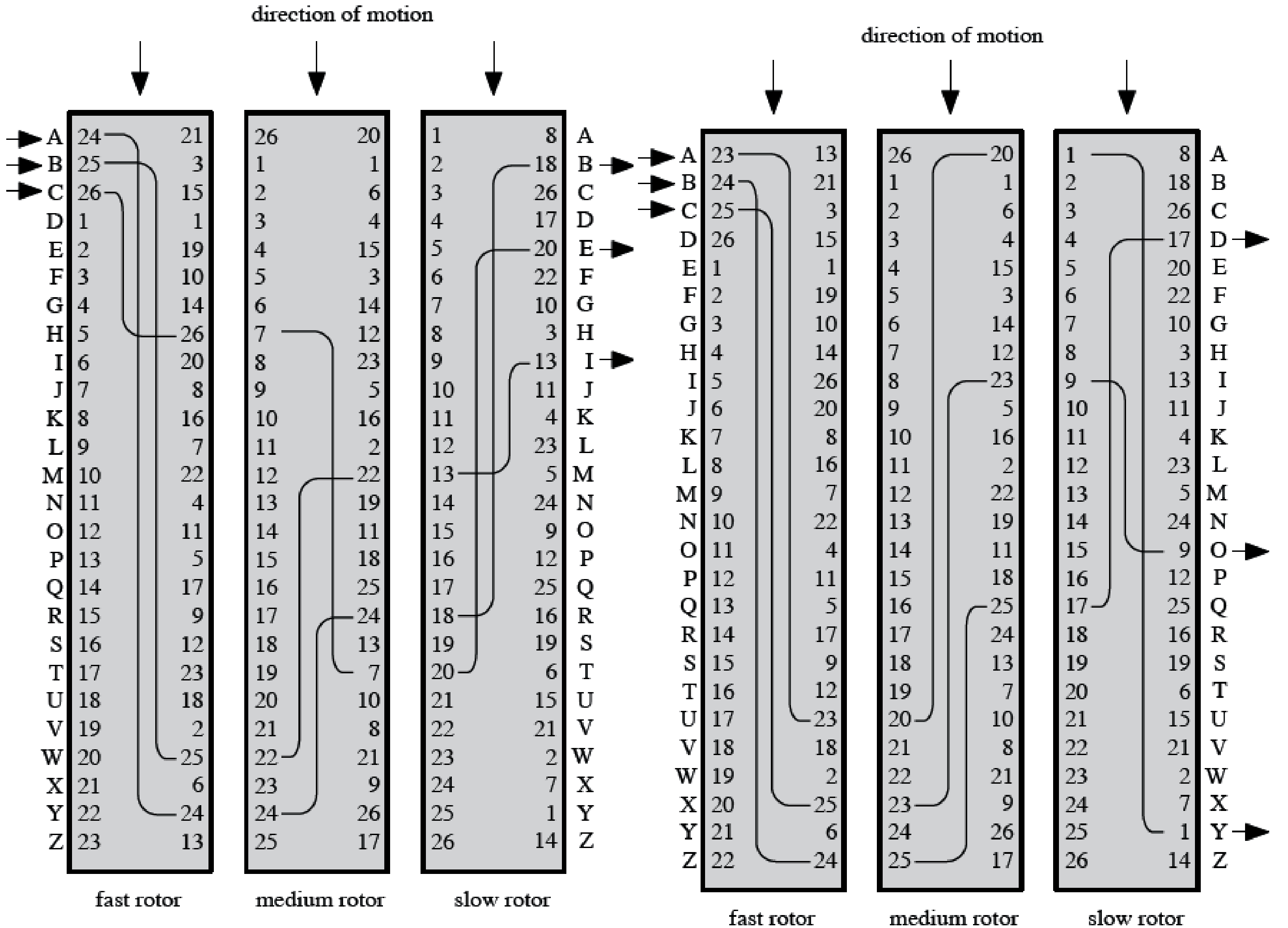
17	09	05	27	24	16	12	07	10	02	22	20	03	25
15	13	04	23	19	14	11	01	26	21	18	08	06	28

Cont'd

- Suggestion: multiple stages of encryption can produce an algorithm that is significantly more difficult to cryptanalyze.
  - This is as true for both *substitution* ciphers and *transposition* ciphers.
  - Example: Rotor machines
    - Machines based on the rotor machine were used by both Germany (Enigma) and Japan (purple) in World War II.

Rotor Machines

- Independently rotating cylinders through which electrical pulses can flow
  ->three-cylinder system
- A polyalphabetic substitution algorithm with a period of 26
  ->26*26*26 substitution alphabets
- DES



(a) Initial setting

(b) Setting after one keystroke

Steganography

- Strictly speaking, not encryption
- Conceal the existence of the message, whereas the methods of cryptography render message unintelligible to outsiders

3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your
letter and for the Summer examination package.
All Entry Forms and Fees Forms should be ready
for final despatch to the Syndicate by Friday
20th or at the very latest, I'm told, by the 21st.
Admin has improved here, though there's room
for improvement still; just give us all two or three
more years and we'll really show you! Please
don't let these wretched 16+ proposals destroy
your basic O and A pattern. Certainly this
sort of change, if implemented immediately,
would bring chaos.

Sincerely yours.

- A puzzle for Inspector Morse (from *The Silent World of Nicholas Quinn*, by Colin Dexter)

Other Steganography Techniques

- Character marking
  - Selected letters of printed or typewritten text are over-written in pencil
  - The marks are ordinarily not visible unless the paper is held at an angle to bright light
- Invisible ink
  - A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper
- Pin punctures
  - Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light
- Typewriter correction ribbon
  - Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light