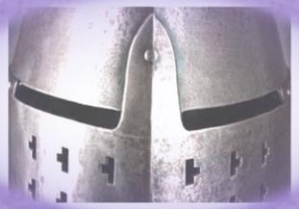


Chapter 3

Classical Encryption Techniques

Definitions

Plaintext

- An original message

Ciphertext

- The coded message

Cryptographic system/cipher

- A scheme

Enciphering/encryption

- The process of converting from plaintext to ciphertext

Deciphering/decryption

- Restoring the plaintext from the ciphertext

Cryptology

- The areas of cryptography and cryptanalysis

=

Cryptography

- The area of study of the many schemes used for encryption

+

Cryptanalysis

- Techniques used for deciphering a message without any knowledge of the enciphering details

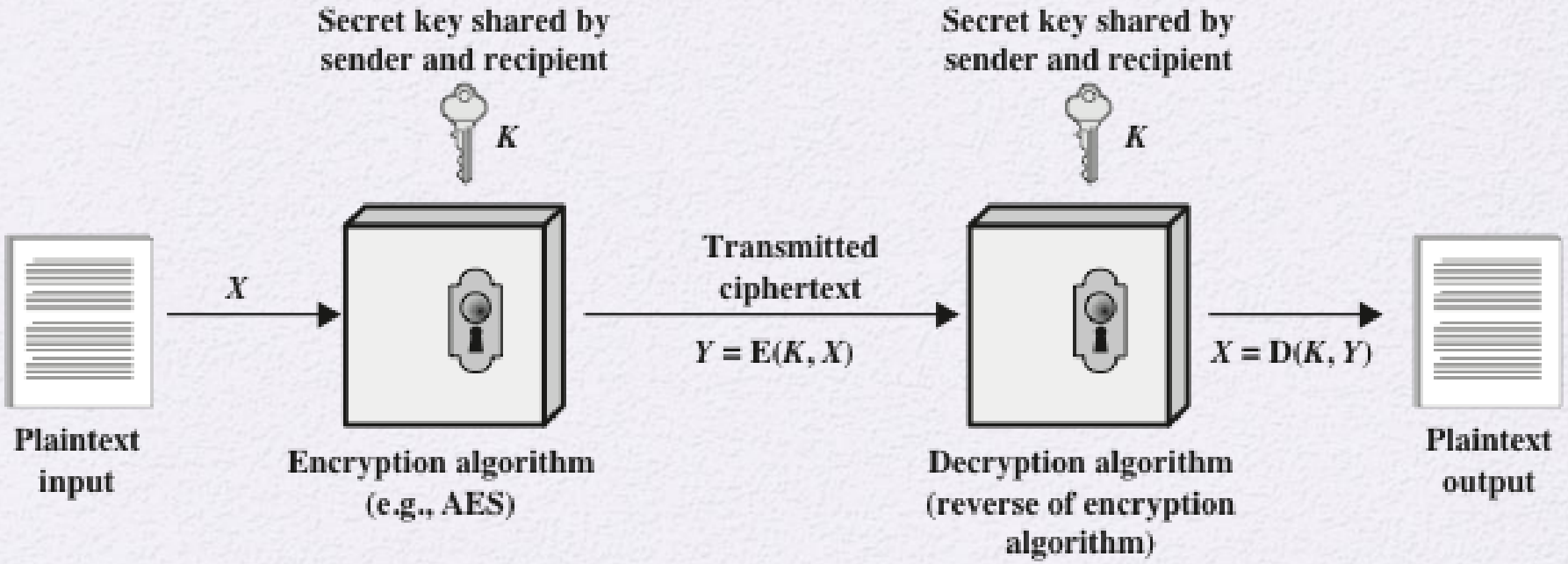


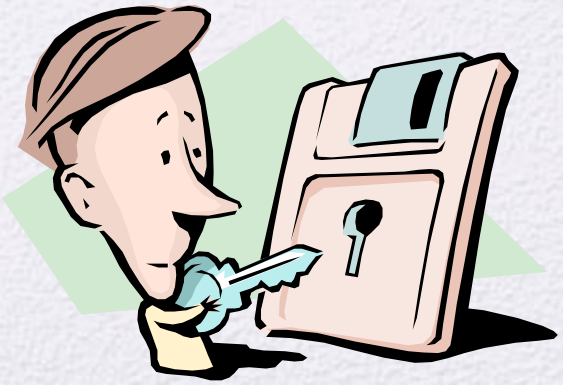
Figure 3.1 Simplified Model of Symmetric Encryption

Symmetric Cipher Model

- There are two requirements for secure use of conventional encryption:

  1. A strong encryption/decryption algorithm

  2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure



Model of Symmetric Cryptosystem : Essential elements of a symmetric encryption scheme

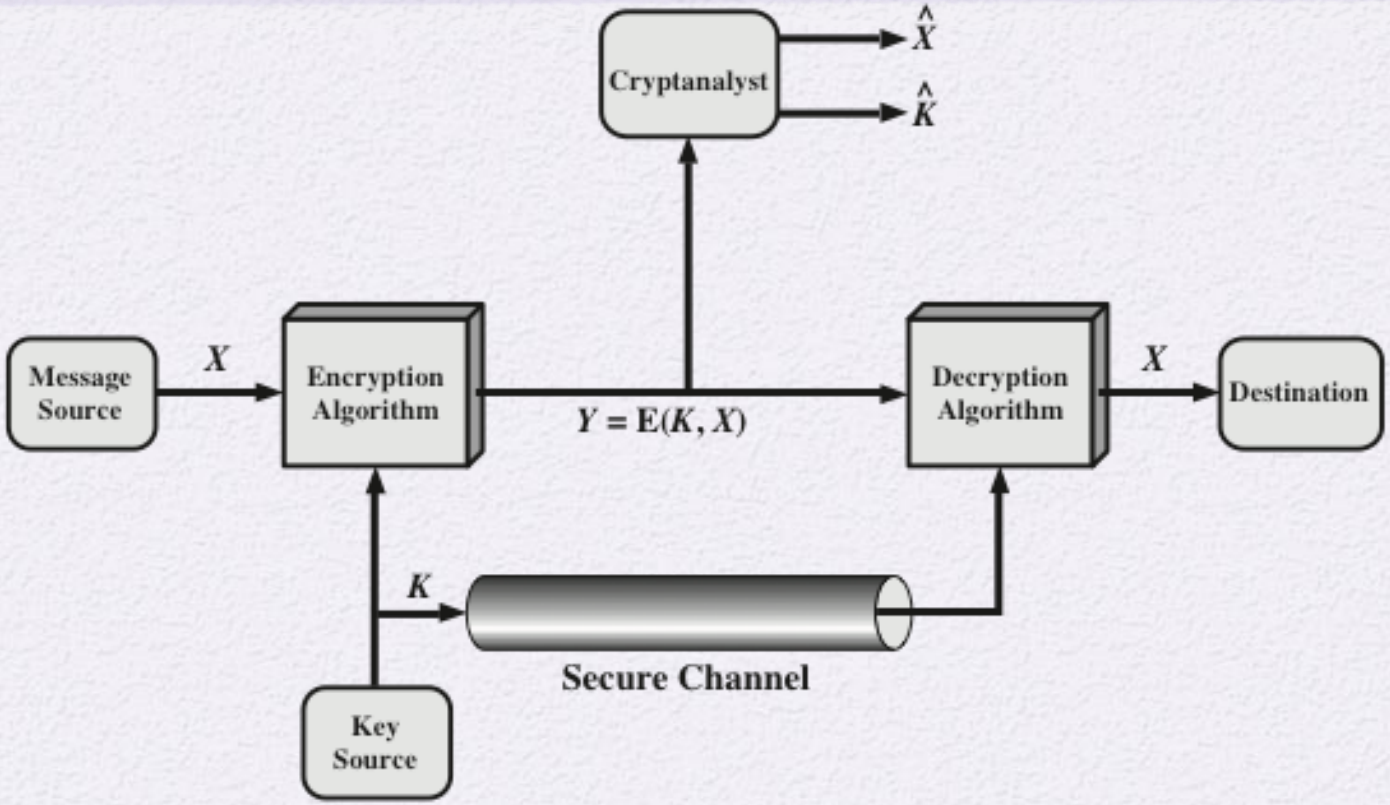
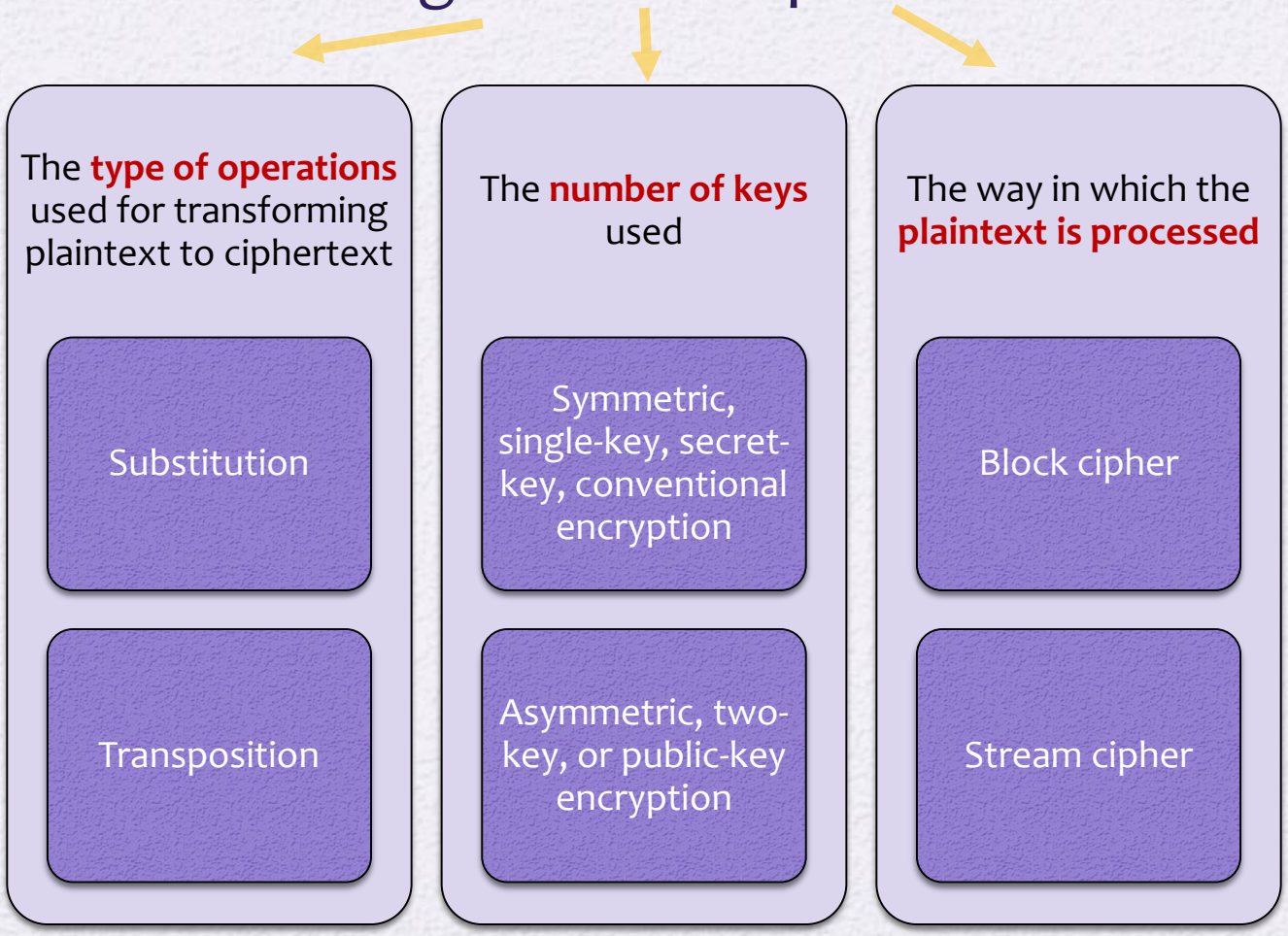


Figure 3.2 Model of Symmetric Cryptosystem

Cryptographic Systems

- Characterized along three independent dimensions:



Approaches to attacking a conventional encryption scheme: Cryptanalysis and Brute-Force Attack

Typically, the objective of attacking an encryption system is to recover the key, rather than simply to recover the plaintext of a single ciphertext.

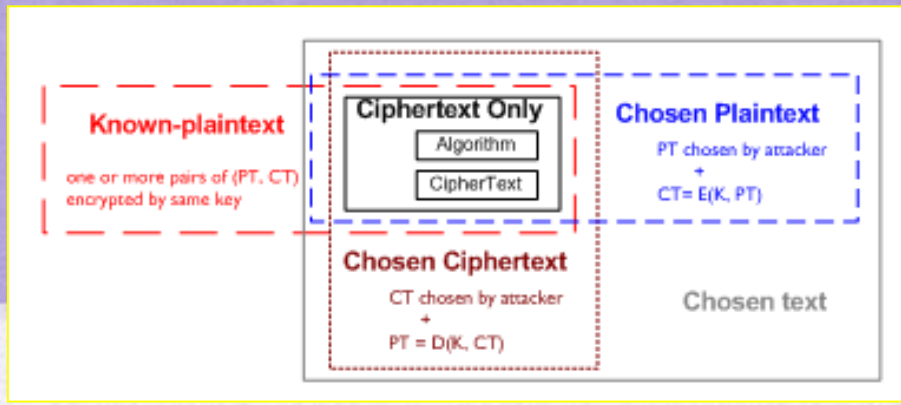
Cryptanalysis

- 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

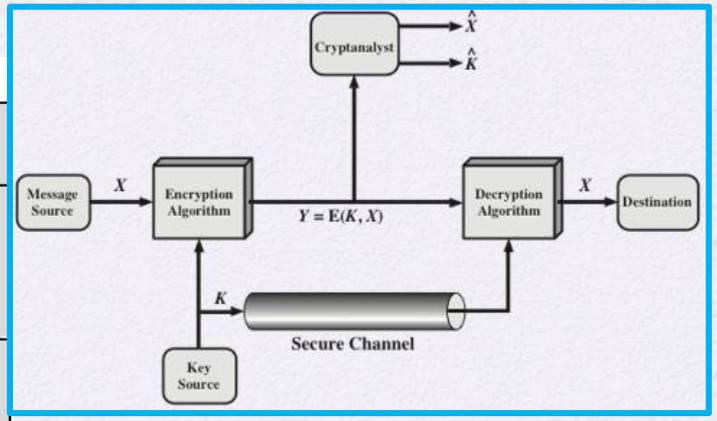
Brute-force attack

- 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

Basic types of Cryptanalyst Attacks



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

- An encryption scheme is unconditionally secure if:
  - the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available.
  - With the exception of a scheme known as the one-time pad (described later in this chapter), there is no encryption algorithm that is unconditionally secure.
- Practically, an algorithm can strive to be computationally secure by meeting one or both of the following criteria:
  - 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

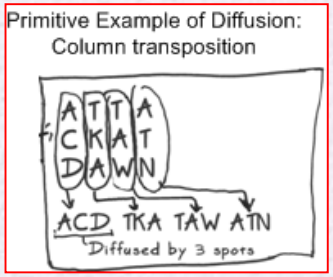
To supplement the brute-force approach, some degree of knowledge about the expected plaintext is needed, and some means of automatically distinguishing plaintext from garble is also needed

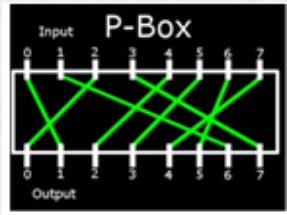
Encryption Goal, Properties and Techniques

- **Goal of Encryption:**
  - Shannon's Strategy
    - If attacker knows statistical analysis about plaintext and ciphertext, then attacker might deduce key or part of it.
    - **The goal of Encryption is:**
      - **To prevent the attacker from figuring out full/part of the key.**
      - **This is done by having statistics of ciphertext independent of plaintext.**
- **Secure Encryption properties**: Confusion and diffusion
  - Confusion and diffusion break the statistical relationship between ciphertext and plaintext/key.
- **Encryption Techniques:** Permutation and Substitution

Two properties of Secure Encryption: Confusion and Diffusion

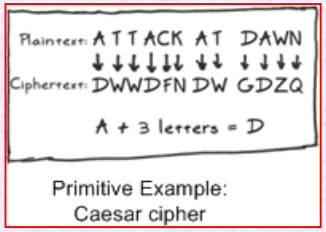
- **Diffusion** seeks to make relationship between (the statistics of) **plaintext** and **ciphertext** as complex as possible.
  - Each bit in plaintext affects many bits in ciphertext.
  - Each bit in ciphertext is affected by many bits in plaintext





P-box is good example of diffusion

- **Confusion** seeks to make relationship between (the statistics of) **ciphertext** and **key** as complex as possible.
  - Even if attacker obtain statistics about ciphertext, attacker cannot deduce information about key.
  - Each character of the ciphertext should depend on several parts of the key.



Primitive Example: Caesar cipher

S-box is good example of confusion

Encryption Techniques

- Substitution:
  - Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.
    - Text format: letters of plaintext are replaced by other letters or by numbers or symbols.
    - Binary format: bits of plaintext are replaced by other bit patterns.
- Permutation (transposition):
  - A sequence of plaintext elements is replaced by a permutation of that sequence, such that the order in which the elements appear in the sequence is changed.

Example Ciphers

- Caesar Cipher
- Monoalphabetic Ciphers
- Playfair Cipher
- Hill Cipher5
- The Hill Algorithm
- Polyalphabetic Ciphers
- Vigenère Cipher
- Vernam Cipher
- One-Time Pad

Caesar Cipher

- Simplest and earliest known use of a substitution cipher
  - Used by Julius Caesar
- Involves 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

Caesar Cipher Algorithm

- 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
```

- Mathematically give each letter a number

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Algorithm can be expressed as:

$$c = E(3, p) = (p + 3) \bmod (26)$$

- A shift may be of any amount, so **that the general Caesar algorithm** is:

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

- Where k takes on a value in the range 1 to 25; the decryption algorithm is simply:

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

Figure 3.3

Brute-Force Cryptanalysis of Caesar Cipher

(This chart can be found on page 75 in the textbook)

Ciphertext

Plaintext

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

Monoalphabetic Cipher

- Recall:
  - Permutation off a finite set of elements S is an ordered sequence of all the elements of S , with each element appearing exactly once.
    - For example, if S = {a, b, c}, there are six permutations of S:
      - abc, acb, bac, bca, cab, cba
    - In general, there are n! permutations of a set of n elements,

- Since there are 26 characters then , then there are 26! possible permutations/keys

- Monoalphabetic *substitution cipher* uses a single cipher alphabet per message. Meaning:
  - "a" is mapped to (for example): c
  - "b" is mapped to : f
  - … etc

- Since there are 26 characters then , then there are 26! possible permutations/keys

Monoalphabetic Cipher: attacks

- If attacker knows the nature of the plaintext (e.g., noncompressed English text), then the attacker can exploit the regularities of the language. For example,
- Attacker can correlate "relative frequency of English letter" to letter frequency in the message.

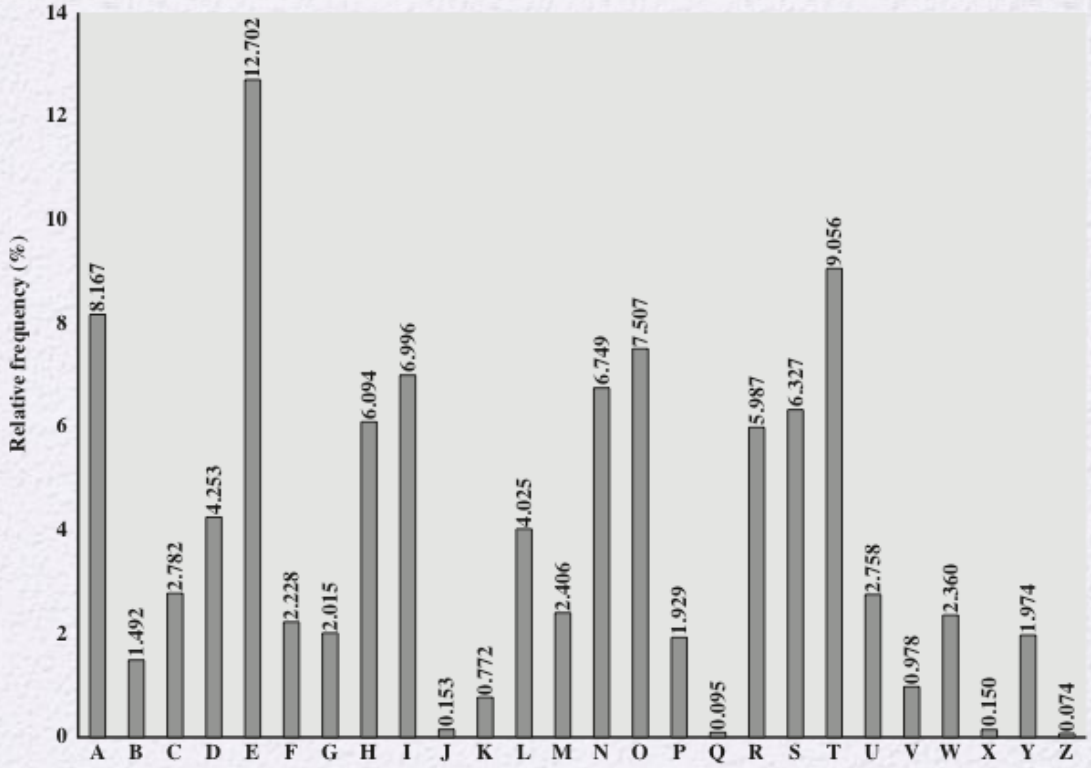


Figure 3.5 Relative Frequency of Letters in English Text

Monoalphabetic Cipher: attack example

- It seems likely that cipher letters P and Z are the equivalents of plain letters e and t, but it is not certain which is which.
- The letters S, U, O, M, and H are all of relatively high frequency and probably correspond to plain letters from the set {a, h, i, n, o, r, s}.
- The letters with the lowest frequencies (namely, A, B, G, Y, I, J) are likely included in the set {b, j, k, q, v, x, z}.

Message

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

Relative Frequencies (%) of Letters

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 Ciphers

- Easy to break because they reflect the frequency data of the original alphabet
- Countermeasure is to provide multiple substitutes (homophones) for a single letter
- Also, a powerful tool is to look at the frequency of two-letter combinations, known as **digrams.**
  - Digram
    - Two-letter combination
    - Most common is *th*
  - Trigram
    - Three-letter combination
    - Most frequent is *the*

Playfair Cipher (read)

- 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
- 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 Key Matrix (read)

- 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

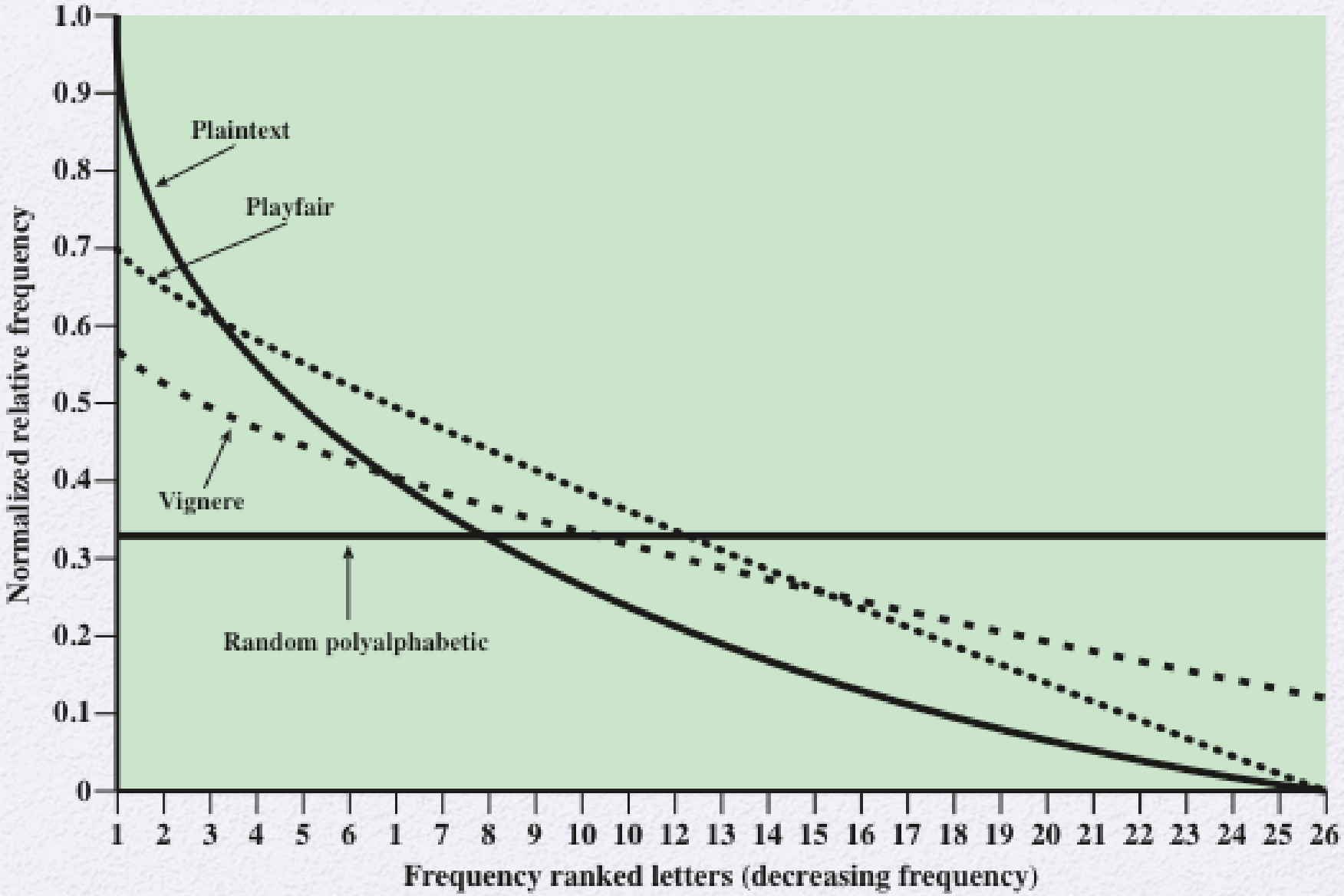


Figure 3.6 Relative Frequency of Occurrence of Letters

Hill Cipher (read)

- 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 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

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

- In this scheme the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25
- To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword

- Mathematically give each letter a number

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

key	=	**W**	**X**	**Y**	**Z**
					(+ mod 26)
plaintext=		**A**	**B**	**C**	**D**
ciphertext=		**W**	**Y**	**A**	**C**

Another Example of Vigenère Cipher

- For example, if the keyword is *deceptive*, the message “we are discovered save yourself” is encrypted as:

```
key:            deceptivewearediscoveredsav
plaintext:      wearediscoveredsaveyourself
ciphertext:     ZICVTWQNGKZEIIGASXSTSLVVWLA
```

Vigenère Autokey System

- The periodic nature of the keyword can be eliminated by using a non-repeating keyword that is as long as the message itself.
- Example:

  key: deceptivewearediscoveredsav

  plaintext: wearediscoveredsaveyourself

  ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA
- 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

Vernam Cipher (stream cipher)

stream cipher= bit by bit

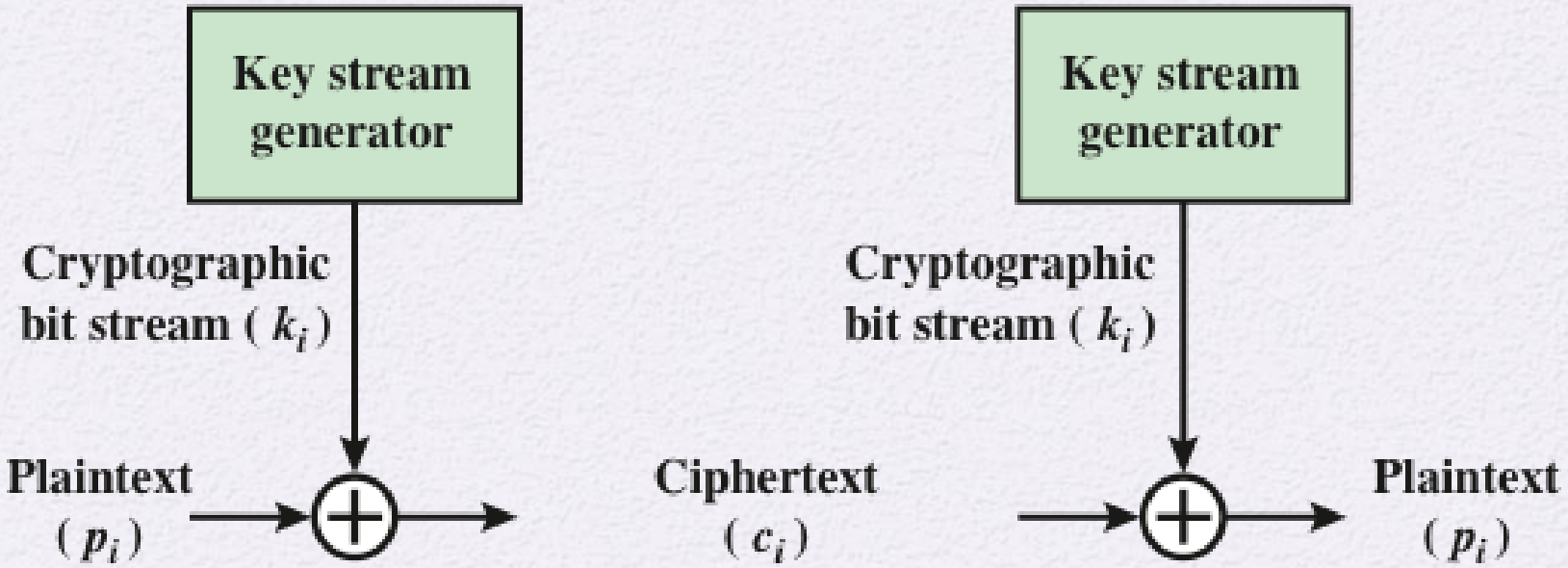


Figure 3.7 Vernam Cipher

One-Time Pad

- This technique uses a key:
  - Key is **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

- The one-time pad is the only cryptosystem that exhibits *perfect secrecy (i.e. unconditionally secure).*

Difficulties

- The one-time pad 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
  - **Significant 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

One-time Pad Example

P: 0 1 1 0 1 1 1

key: 1 0 1 1 0 1 0 ⊕

C: 1 1 0 1 1 0 1

Rail Fence Cipher (read)

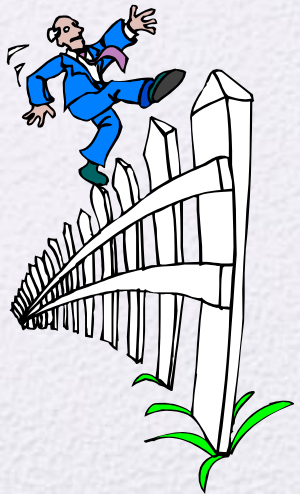
- Simplest transposition cipher
- Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows
- To encipher the message "meet me after the toga party" with a rail fence of depth 2, we would write:

  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 (read)

- Is a more complex transposition
- 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

(read)

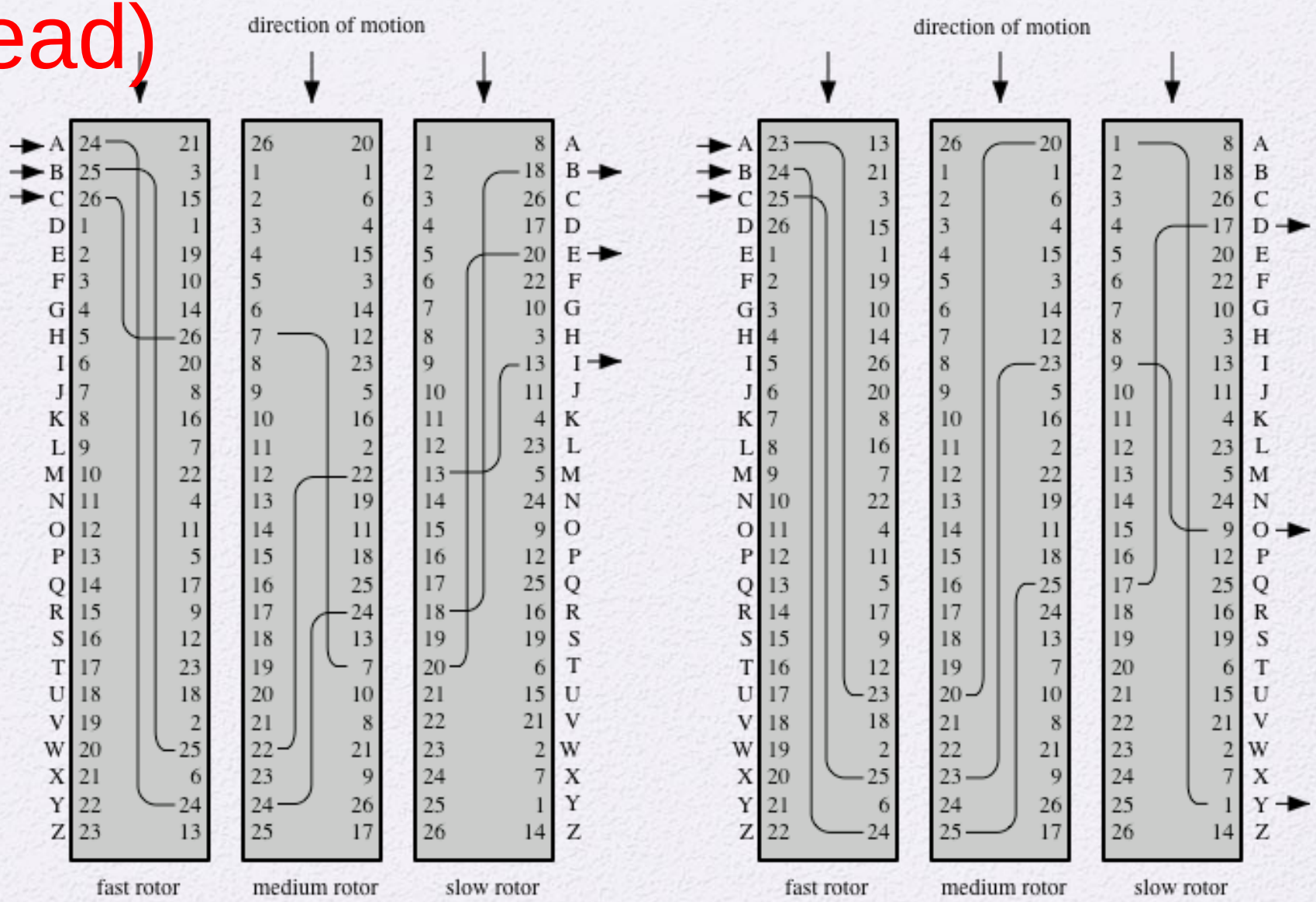


Figure 3.8 Three-Rotor Machine With Wiring Represented by Numbered Contacts

Steganography

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)

Steganography vs. Encryption

- Steganography has a number of drawbacks when compared to encryption
  - It requires a lot of overhead to hide a relatively few bits of information
  - Once the system is discovered, it becomes virtually worthless

- The advantage of steganography
  - It can be employed by parties who have something to lose should the fact of their secret communication (not necessarily the content) be discovered
- Encryption flags traffic as important or secret or may identify the sender or receiver as someone with something to hide

Summary

- Symmetric Cipher Model
  - Cryptography
  - Cryptanalysis and Brute-Force Attack
- Transposition techniques
- Rotor machines

- Substitution techniques
  - Caesar cipher
  - Monoalphabetic ciphers
  - Playfair cipher
  - Hill cipher
  - Polyalphabetic ciphers
  - One-time pad
- Steganography