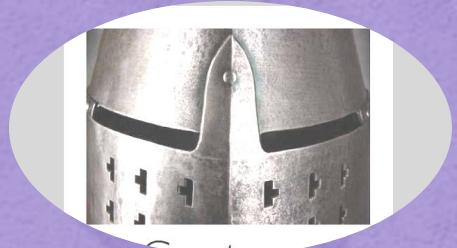


# Cryptography and Network Security

---

Sixth Edition  
by William Stallings



Courtesy

# Chapter 2

---

## Classical Encryption Techniques

*"I am fairly familiar with all the forms of secret writings, and am myself the author of a trifling monograph upon the subject, in which I analyze one hundred and sixty separate ciphers," said Holmes.*

*—The Adventure of the Dancing Men,  
Sir Arthur Conan Doyle*

# Symmetric Encryption

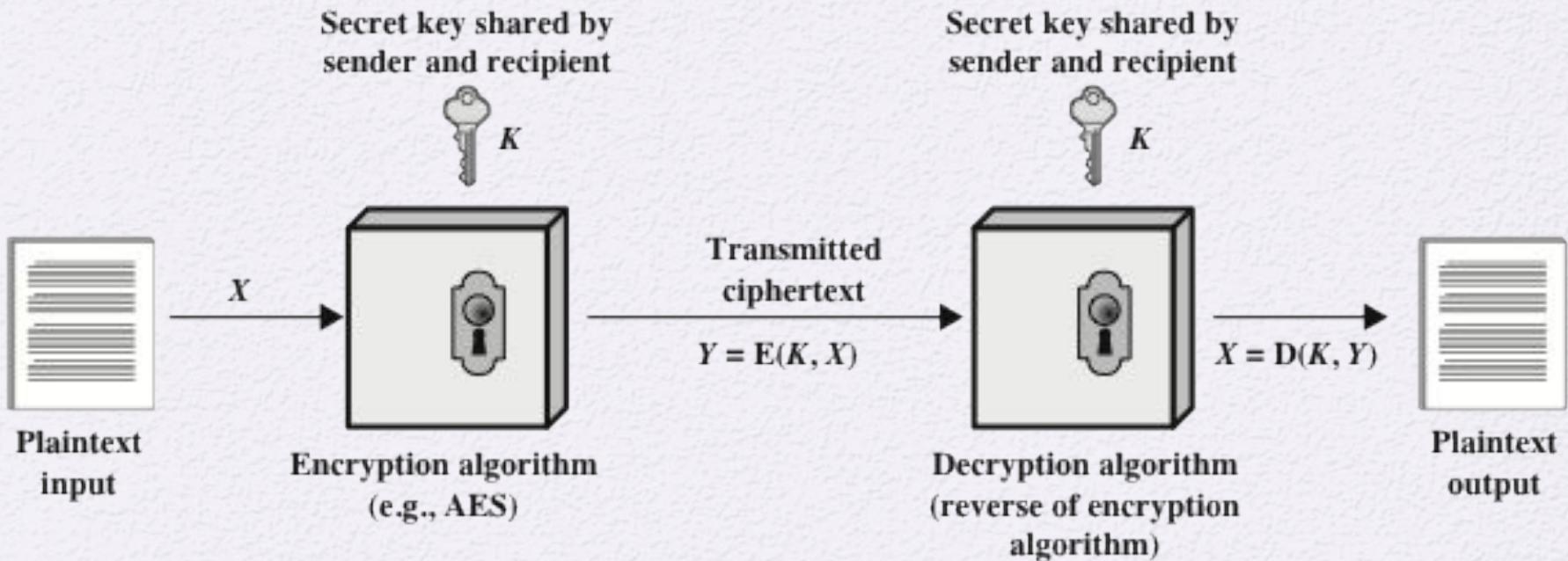
- Also referred to as conventional encryption or single-key encryption
- Was the only type of encryption in use prior to the development of public-key encryption in the 1970s
- Remains by far the most widely used of the two types of encryption



# Basic Terminology

- 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

# Simplified Model of Symmetric Encryption



**Figure 2.1 Simplified Model of Symmetric Encryption**

# Model of Symmetric Cryptosystem

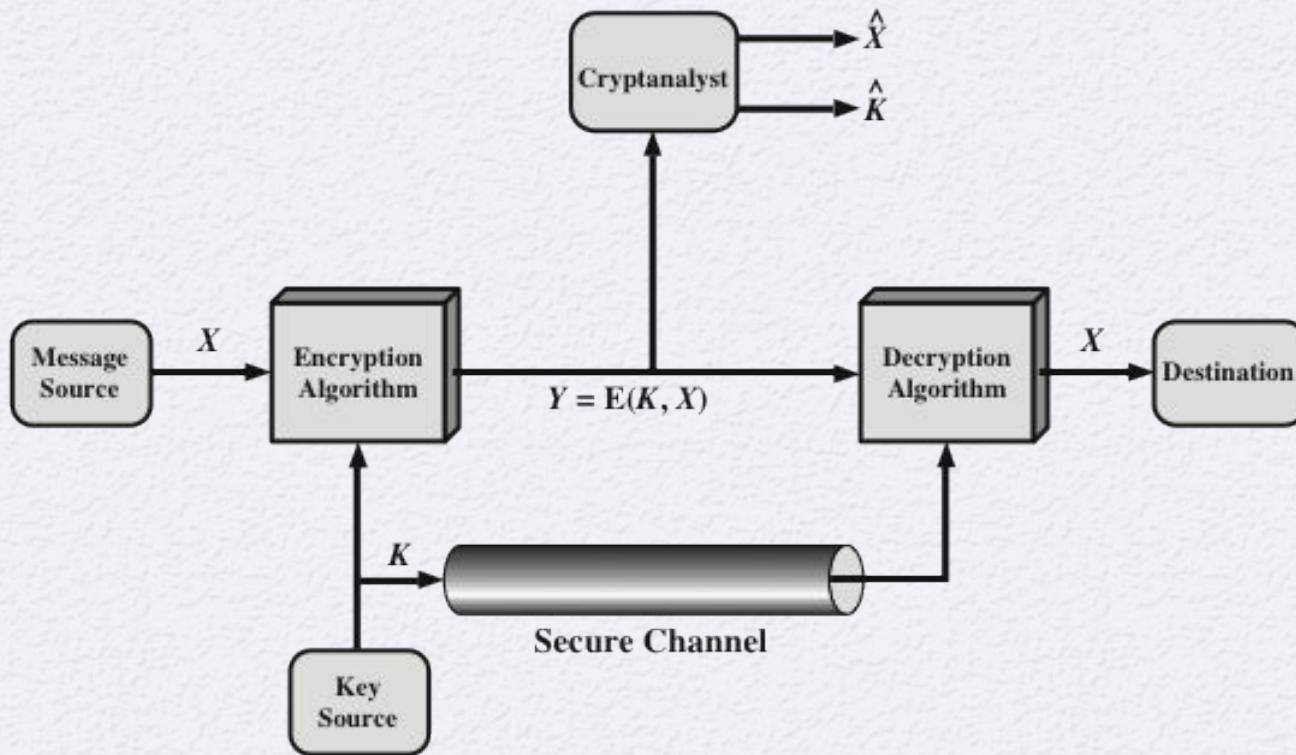


Figure 2.2 Model of Symmetric Cryptosystem

# Cryptographic Systems

- Characterized along three independent dimensions:

# Cryptanalysis and Brute-Force Attack

**Table 2.1**

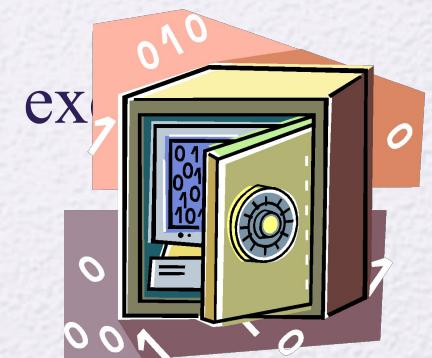
Types of Attacks

on Encrypted Messages

Type of Attack	Known to Cryptanalyst
Ciphertext Only	<ul style="list-style-type: none"><li>• Encryption algorithm</li><li>• Ciphertext</li></ul>
Known Plaintext	<ul style="list-style-type: none"><li>• Encryption algorithm</li><li>• Ciphertext</li><li>• One or more plaintext-ciphertext pairs formed with the secret key</li></ul>
Chosen Plaintext	<ul style="list-style-type: none"><li>• Encryption algorithm</li><li>• Ciphertext</li><li>• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key</li></ul>
Chosen Ciphertext	<ul style="list-style-type: none"><li>• Encryption algorithm</li><li>• Ciphertext</li><li>• Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key</li></ul>
Chosen Text	<ul style="list-style-type: none"><li>• Encryption algorithm</li><li>• Ciphertext</li><li>• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key</li><li>• Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key</li></ul>

# Encryption Scheme Security

- 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
- Computationally secure
  - 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

# Substitution Technique

- 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





# 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:

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

# Brute-Force Cryptanalysis of Caesar Cipher

(This chart can be found on page 35 in the textbook)

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 ydrcc 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	vnnn vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tilla 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

Figure 2.3 Brute-Force Cryptanalysis of Caesar Cipher

# Sample of Compressed Text

-+Wu"- Ω-0)≤4{==‡, ē-Ωtrāu.-f ◊-z-  
Ü#20#λαδ ε≈q7,Ωn-@3N0Ü Ωz'Y-f≈f [±0\_ èΩ,<NO-†«"xā λεεèu3λ  
x}ö5k=λ  
\_yí "Δέ] . n J//iT&&1 'c<uΩ-  
ÄD(G WÄC-y\_iöÄM PÖ1<îÜtç], n; "i^uññ"="L" 9OgflO" &Ø≤ -≤ φö5":  
"ε!SGqévo" ú\,S>h<-\*6ø†%x' " |ñó#="myk" ≥flP<,fi Áj ÅöL"zù-  
Ω"ö"6øy(‡ ,Ωöö .i π=Ái "ú02çSy' o-  
2Änisi /8^"ΠK\*\*PÖñ,úé^'3Σ"o"öZì"Y-?ΩmY> Ω+øö/ ' <KfL\*\*"50"  
B ZeK"Qßyüf, !öñfzss/] >EQ u

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
- If the “cipher” line can be any permutation of the 26 alphabetic characters, then there are  $26!$  or greater than  $4 \times 10^{26}$  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

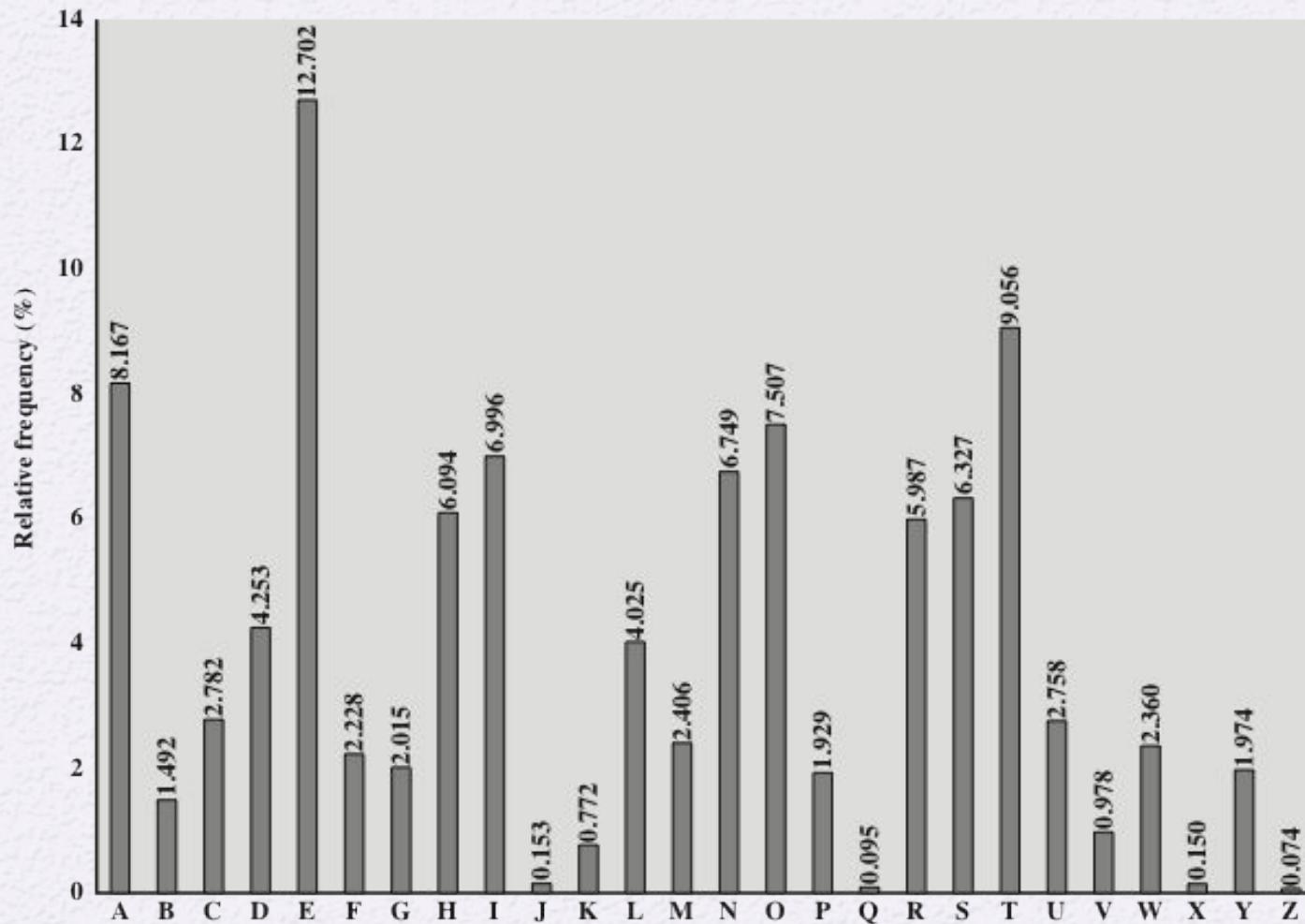
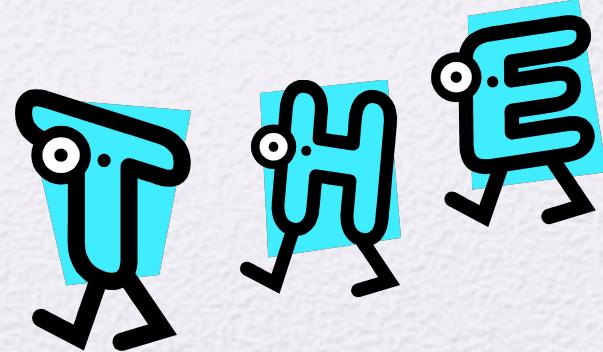
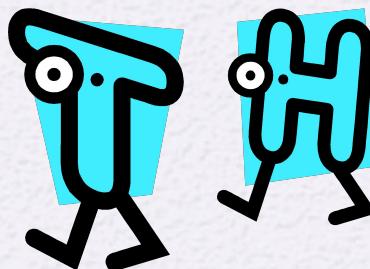


Figure 2.5 Relative Frequency of Letters in English Text

# 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
- Digram
  - Two-letter combination
  - Most common is *th*
- Trigram
  - Three-letter combination
  - Most frequent is *the*



# 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  $5 \times 5$  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

- 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

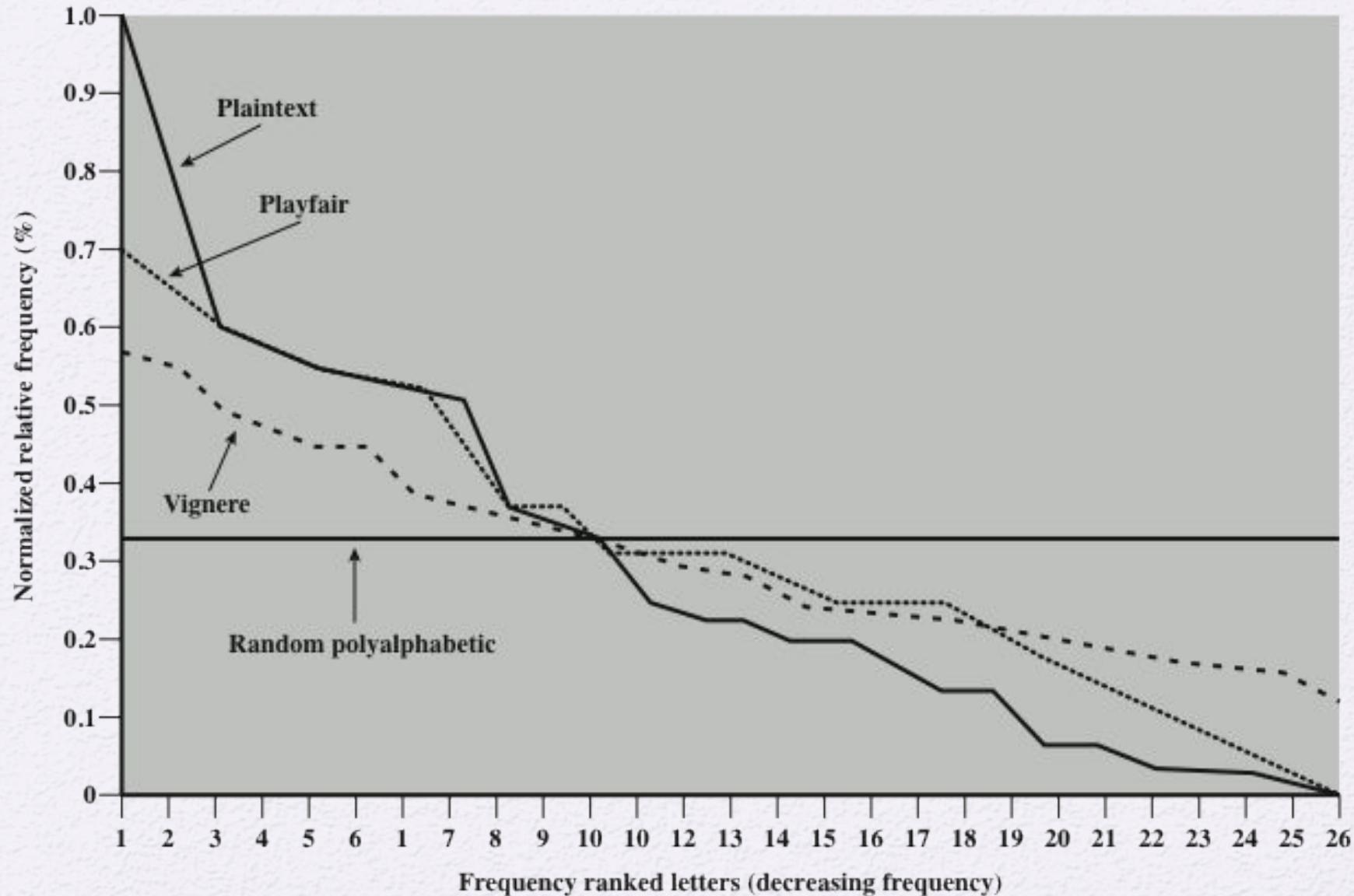


Figure 2.6 Relative Frequency of Occurrence of Letters

# Hill Cipher

- 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  $3 \times 3$  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

# Vigenère Cipher

- 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

# 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:           deceptive deceptive deceptive

plaintext:    wearediscoveredsaveyourself

ciphertext:

ZICVTWQNGRZGVTWAVZHCQYGLMGJ

# Vigenère Autokey System

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

- 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

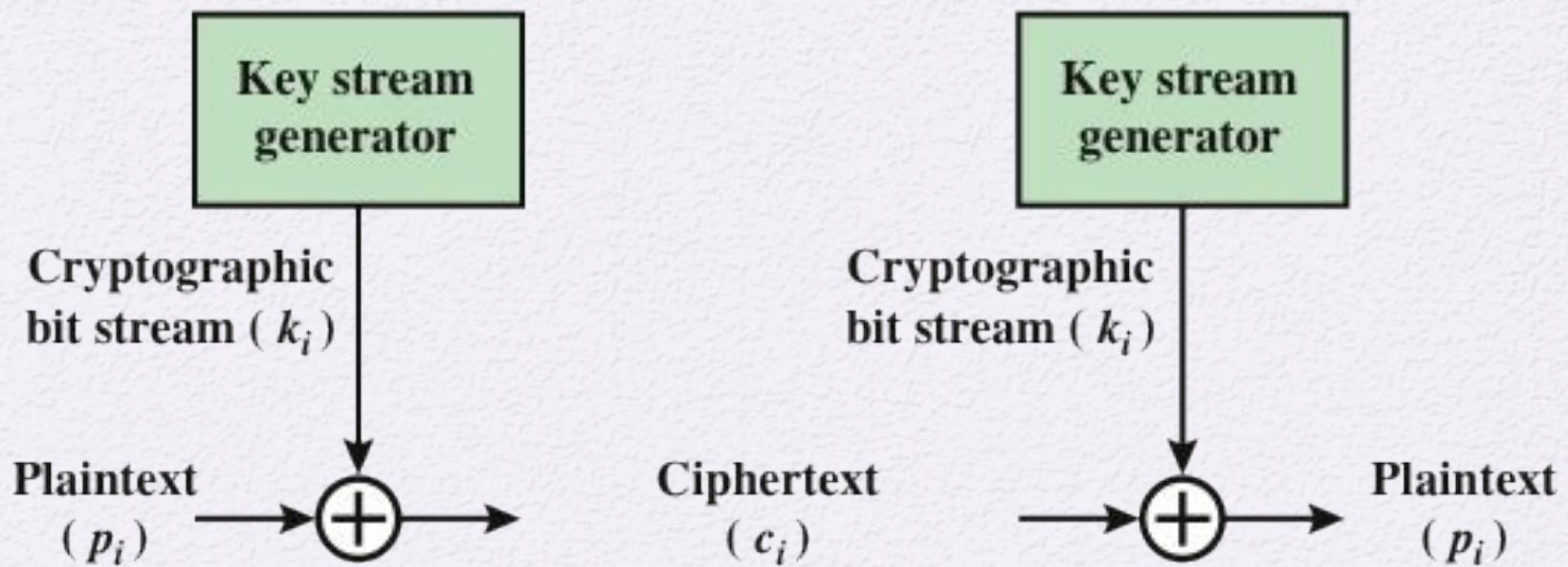


Figure 2.7 Vernam Cipher

# One-Time Pad

- 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* (see Appendix F)

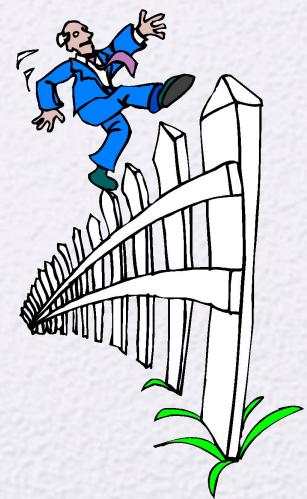
# Rail Fence Cipher

- 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

- 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

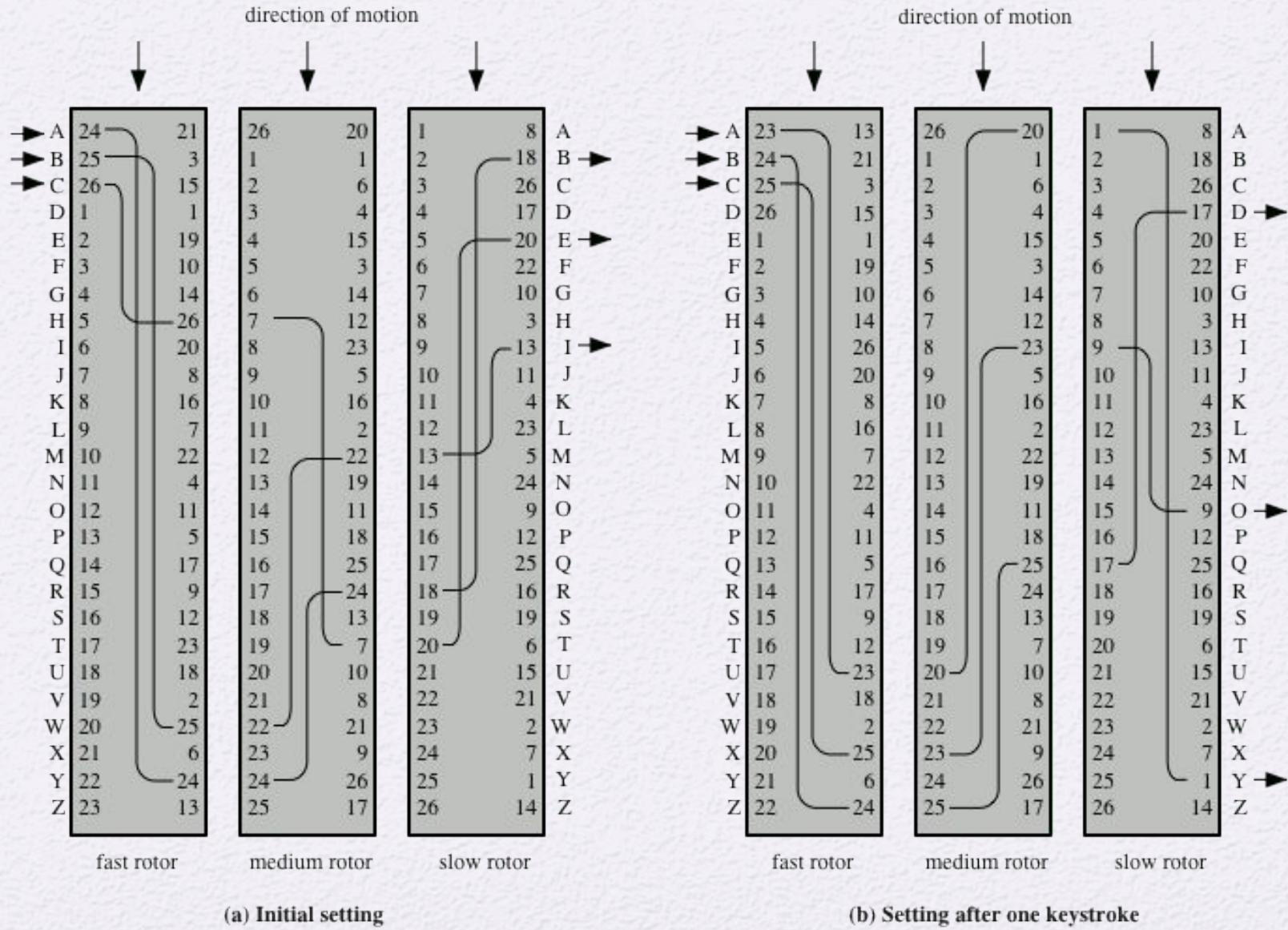
Plaintext:

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:

TTNAAPTMUOAODWCOIXKNLYPETZ

# Rotor Machines



**Figure 2.8 Three-Rotor Machine With Wiring Represented by Numbered Contacts**

# Steganography

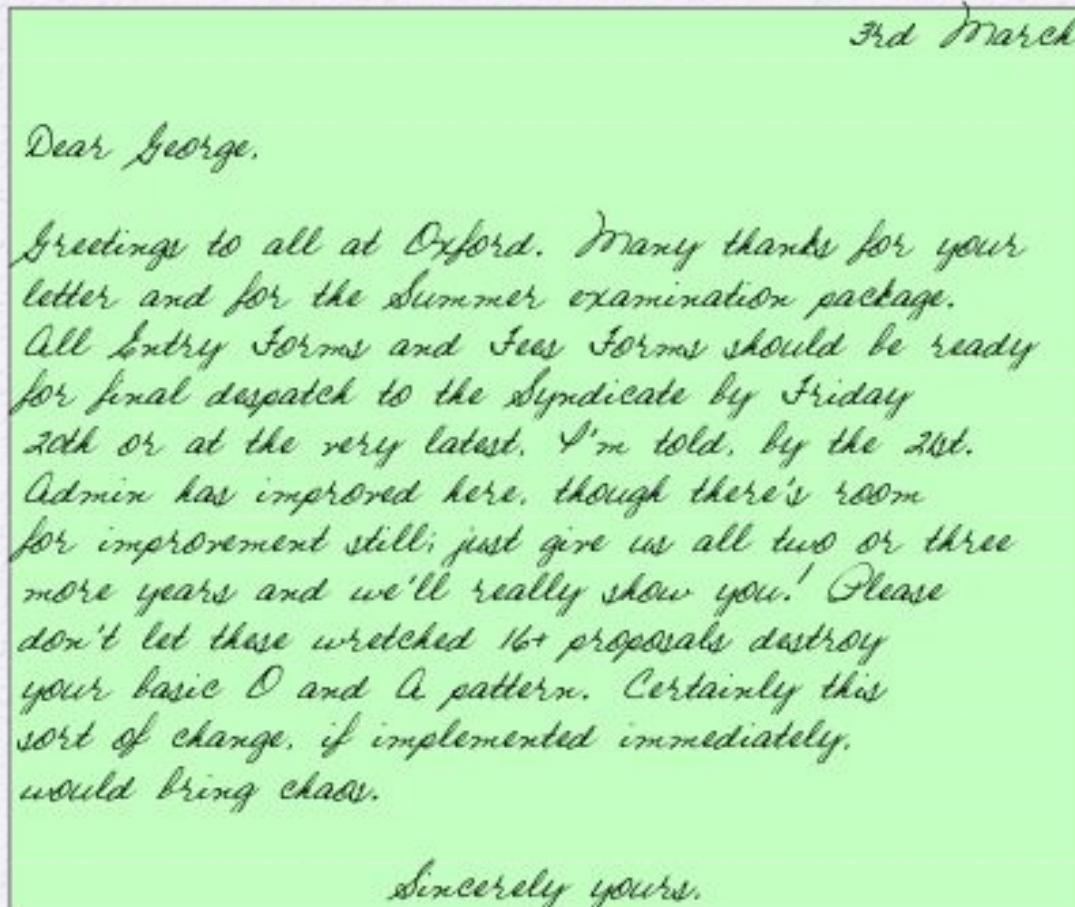


Figure 2.9 A Puzzle for Inspector Morse  
(from *The Silent World of Nicholas Quinn*, by Colin Dexter)

# 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

# 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

