



Chapter 3

Classical Encryption Techniques

Definitions

- Plaintext: an original message
- Ciphertext: the coded message
- Enciphering/encryption: the process of converting from plaintext to ciphertext
- Deciphering/decryption: restoring the plaintext from the ciphertext
- Cryptographic system/cipher: a scheme of encryption and decryption

Definitions

- Cryptography: the study of schemes used for encryption and decryption
- Cryptanalysis: the study of deciphering messages without details of secrets (破譯)
- Cryptology: the areas of cryptography and cryptanalysis

Cryptographic Systems

Three aspects

- Ways of transforming plaintext to ciphertext
 - Substitution
 - Transposition
- Number of keys
 - One-key: symmetric, conventional
 - Two keys: asymmetric, public-key, modern
- Ways of processing plaintexts
 - Block cipher: information processing
 - Stream cipher: communication

Attacks

- Cryptanalysis
 - Analyze and exploit the cipher algorithm with some knowledge about the plaintext and ciphertext
 - Attempt to deduce a specific plaintext or the used key
- Brute-force attack
 - Use computing power to try 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

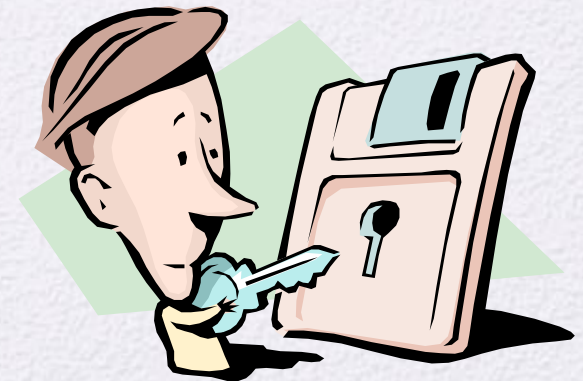
Type of Attack	Known to Cryptanalyst
Ciphertext Only	<ul style="list-style-type: none"> • Encryption algorithm • Ciphertext
Known Plaintext	<ul style="list-style-type: none"> • Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	<ul style="list-style-type: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

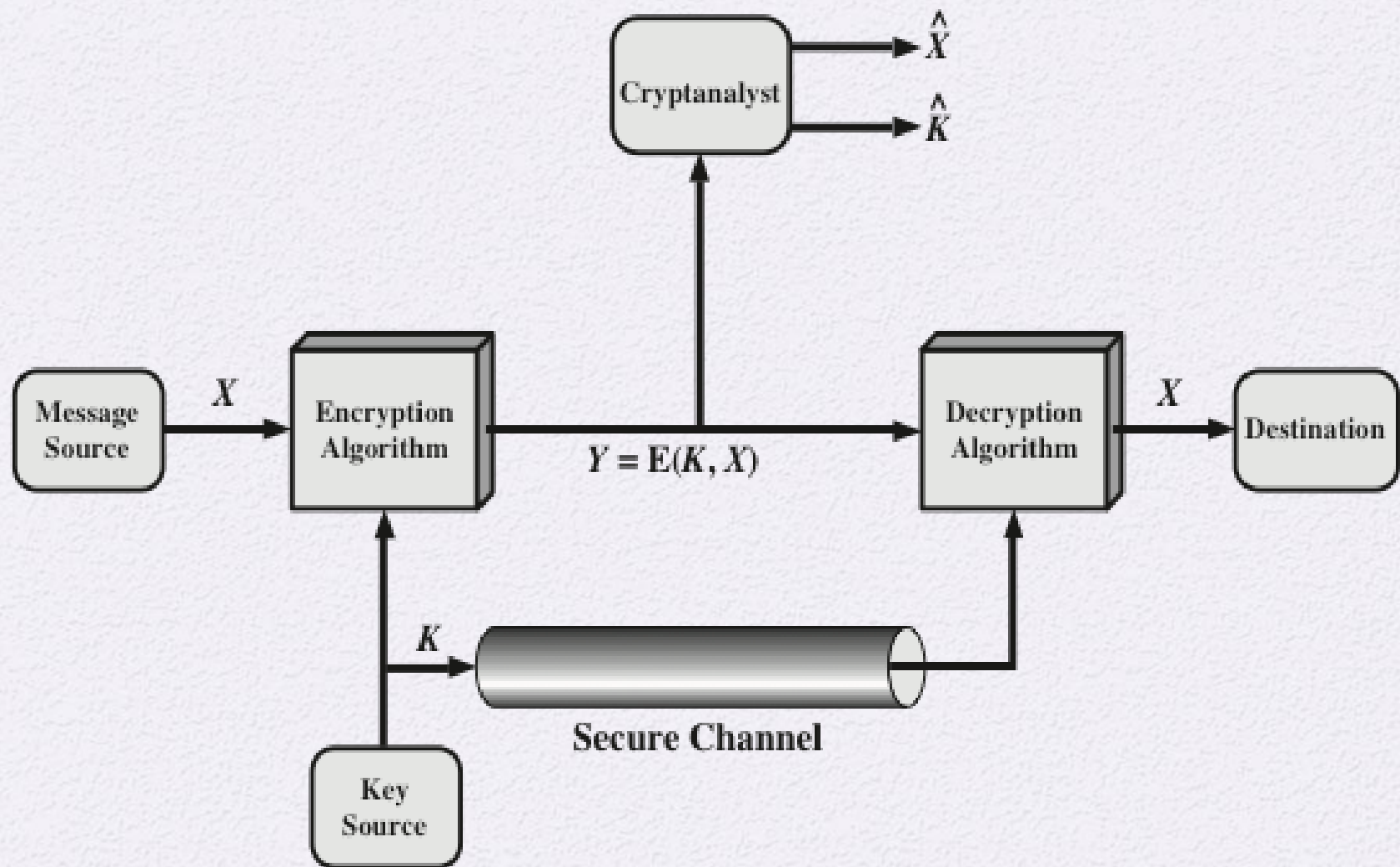
Encryption Scheme Security

- Unconditionally/perfectly secure
 - No matter how much time an opponent has, it is impossible 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

Symmetric Cipher Model

- The strong encryption/decryption algorithms are publicly known
- The sender and the receiver obtain the same secret key in a secure fashion and keep the key secure







Caesar Cipher



- Simplest and earliest known use of a substitution cipher
- $A \rightarrow D, B \rightarrow E, \dots, W \rightarrow Z, X \rightarrow A, Y \rightarrow B, Z \rightarrow C$

plain: meet me after the toga party

cipher: PHHW PH DIWHU WKH WRJD SDUWB

Caesar Cipher Algorithm

- 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

- Encryption: k is the key, $1 \leq k \leq 25$

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

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

Brute-Force Cryptanalysis of Caesar Cipher

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	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	hsjlg
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

OK for Compressed Text

- Caesar cipher can be used to encrypt compressed texts which contain no recognizable/meaningful words

```
~+Wu"- Q-O)S4(=+ , e-Q#rau.-i 0-Z-  
U#20#Aed e=q7,Qn-@3N0U Qz'Y-f=i[±0_ èQ,<NO-t«"xã  Aafèu3A  
x)85k°Å  
_yí 'ΔÉ) ,= J/'iTê&1 'c<uQ-  
AD(G WAC~y_I8AW P01=iU+ç|,=,~i^uRn~="L"9OgflO~&ES ~S ø05":  
"E!SQqèvo" ú\,S>h<-*6ø±8x'"|fio#="myk~znP<,fi Áj A0_L~Zù-  
Q"0"6ay{8 ,Q8ó ,i π+Ái'ú02çsy'O-  
2ÅnBi /@~"[]K**PQπ,ú6^'3Σ~ø"0zi~Y-YQmY> Q+eð/'<Kf_L*+~"S0~  
B ZeK"Q8yUf,i0nIzaS/)»BQ u
```

Figure 2.4 Sample of Compressed Text

Monoalphabetic Cipher

| to |

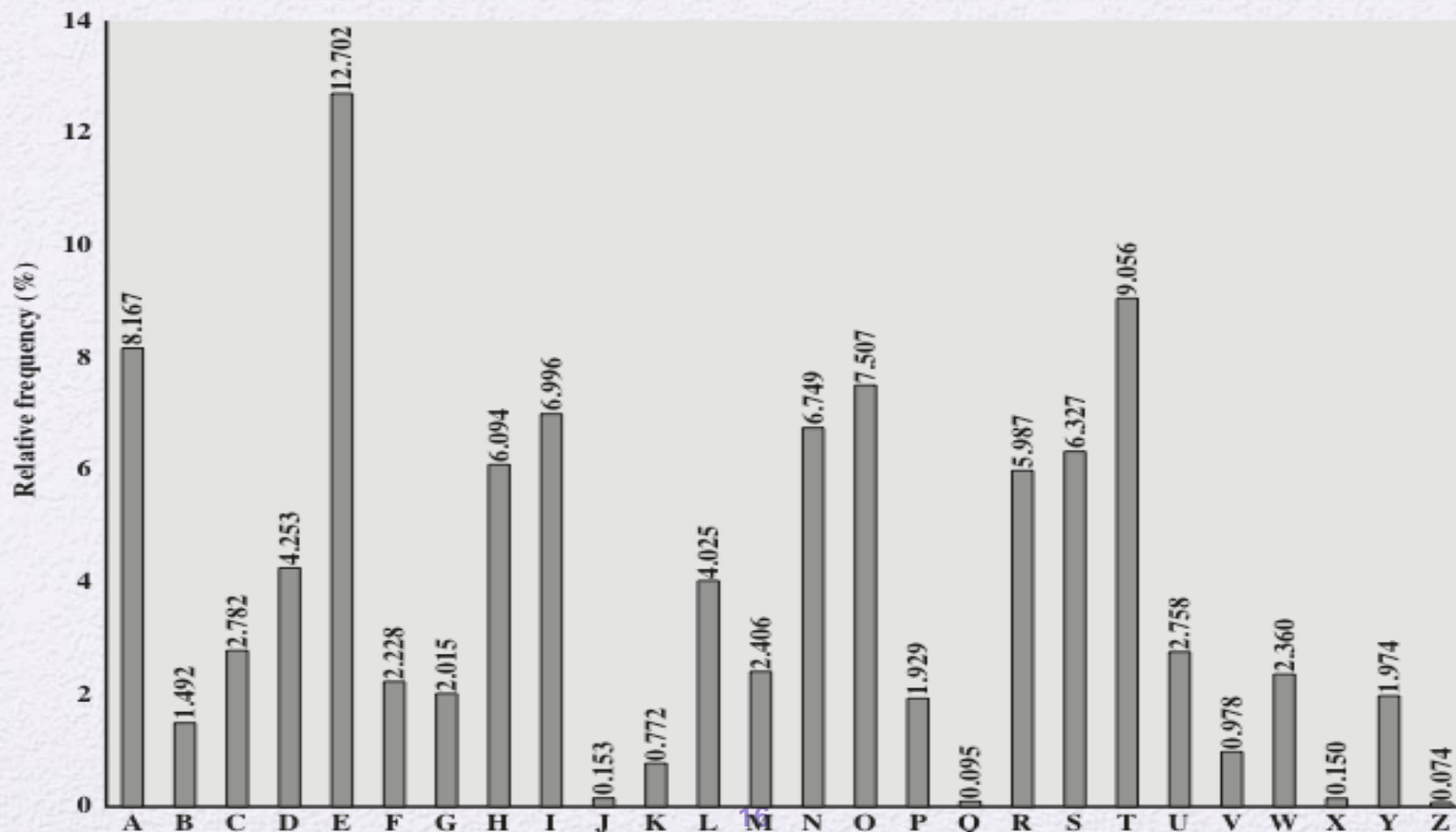
- A substitute (permutation): one-to-one mapping
 - $A \rightarrow R, B \rightarrow L, \dots$
- There 26! possible keys, greater than 4×10^{26} possible keys
- Also called monoalphabetic substitution cipher

Example: ciphertext

- KVFNO OGMDD QBKSE BKRSN CKMKG QYQKC SFBFA NTEJB ABYIB QKGQE
TRKAQ BGKYF SMTJJ SFBEG DDBRS OKRRB MDBQK GQOJK MBSFB VNQJA
FKRBU BQIMN VMGRK MGYMQ BAGEJ BRGDF SVFBS FBQNM JKMAN QGMSF
BKGQR TYFDQ KUGSX ABCXG MDOQN ONQSG NMRYN LEGMB AVGSF SFBDB
MTGMB JXBMH NXKEJ BBWOB QGBMY BNCCJ XGMDG MNMBF KUBVN MGSJB
DGNMR NCKAL GQBQR RGMYP GSRCG QRSYN LLBQY GKJUN XKDBG MZVBG
MTJJM TJJRG BEBMR NGSVK RMNRT QOQGR BSFKS SFBQB VKRVG ABROQ
BKAYN MRSBQ MKSGN MKSSF BCBEQ TKQXB GMRUG BQKMM NTMYB LBMSS
FKSKG QETRG MSBMA RSNYB KRBOQ NATYS GNMNC SFBKA QBGKY FSMTJ
JGMZV BGMTJ JBGMR MBTMB CCBYS GUBJX OJKYG MDKMB WOGQX AKSBN
MKMKG QYQKC SSFKS VKRNM YBRBB MKRSF BCTST QBNCK UGKSG NMETS
FNVPT GYIJX KQBKA QBGKY FSMTJ JRDNG MDSNU KMGRF CQNLN TQRIG
BRGRV GABRO QBKAK CCBYS GNMCM QSFBF TDBKG QYQKC SBMNT DFSNI
BBOGS CJXGM DVBJJ GMSNG SRANS KDBGM SFBVK XLKMX YJKRR GYOJK
MBRYN MSGMT BCJXG MDVBJ JEBXN MASFB GQRBQ UGYBJ GCB

Security problem

- Letter frequencies are un-balanced in normal texts.



Attack: Frequency count

- A:20 **B:93** C:22 D:20 E:12
F:30 **G:70** H:1 I:5 J:34
K:59 L:7 **M:68** N:45 O:15
P:1 Q:47 R:42 **S:56** T:24
U:9 V:17 W:2 X:15 Y:27 Z:2
- **Inference:** {B, G, K, M, S} \rightarrow {A, E, I, N, O, T}

Further observation

- “th”: the highest frequency of two letter combination
- sf: 15
 - $\text{sf} \rightarrow \text{th}$
- “the”, “that” occur often
 - $\text{sfb} \rightarrow \text{the}$
 - ...

Example: Plaintext

- **A** whopp**in**g gre**at** beast of an aircraft, **th**e double-decker Airbus A380 -- the biggest passenger airplane the world has ever known -- is an incredible sight whether on land or in the air.

Such gravity-defying proportions combined with the genuinely enjoyable experience of flying in one have won it legions of admirers since its first commercial voyage in 2007.

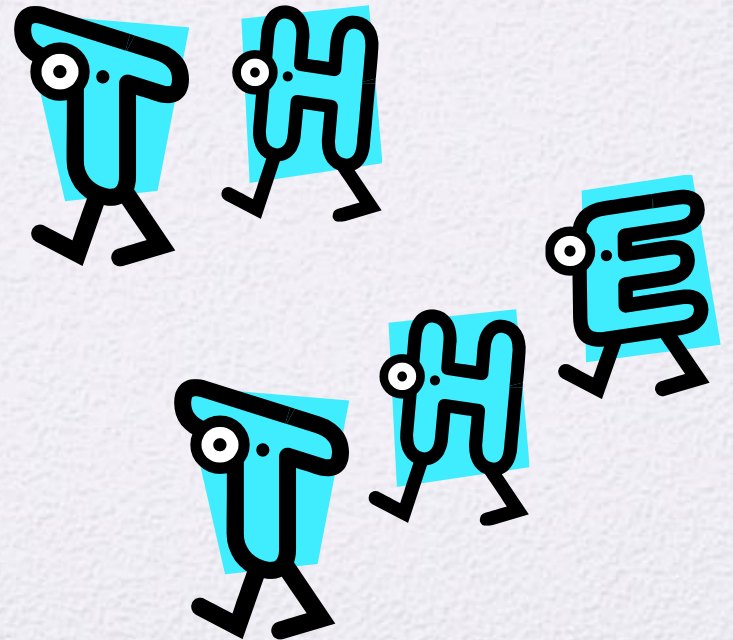
So it was no surprise that there was widespread consternation at the February 14 announcement that Airbus intends to cease production of the A380 in 2019, effectively placing an expiry date on an aircraft that was once seen as the future of aviation.

But how quickly are A380s going to vanish from our skies? Is widespread affection for the huge aircraft enough to keep it flying well into its dotage, in the way many classic planes continue flying well beyond their service life?

- **Note: spaces and special characters are omitted in encryption.**

Weakness

- Easy to break: use the frequency data of the original alphabet
- Countermeasure: multiple substitutes (homophones) for a single letter
- Digram ^{1字对多字}
 - Two-letter combination
 - Most common is *th*
- Trigram
 - Three-letter combination
 - Most frequent is *the*



Playfair Cipher

2 to 2

- Multiple-letter encryption cipher
- Key: a 5 x 5 matrix of letters
- 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
- Example: 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

Example

- $mn \rightarrow OA$, $ny \rightarrow YG$, $eq \rightarrow GL$, $pi \rightarrow SF$
- at ta ck at fo ur pm
 \rightarrow RS SR DE RS PH ZM LO

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

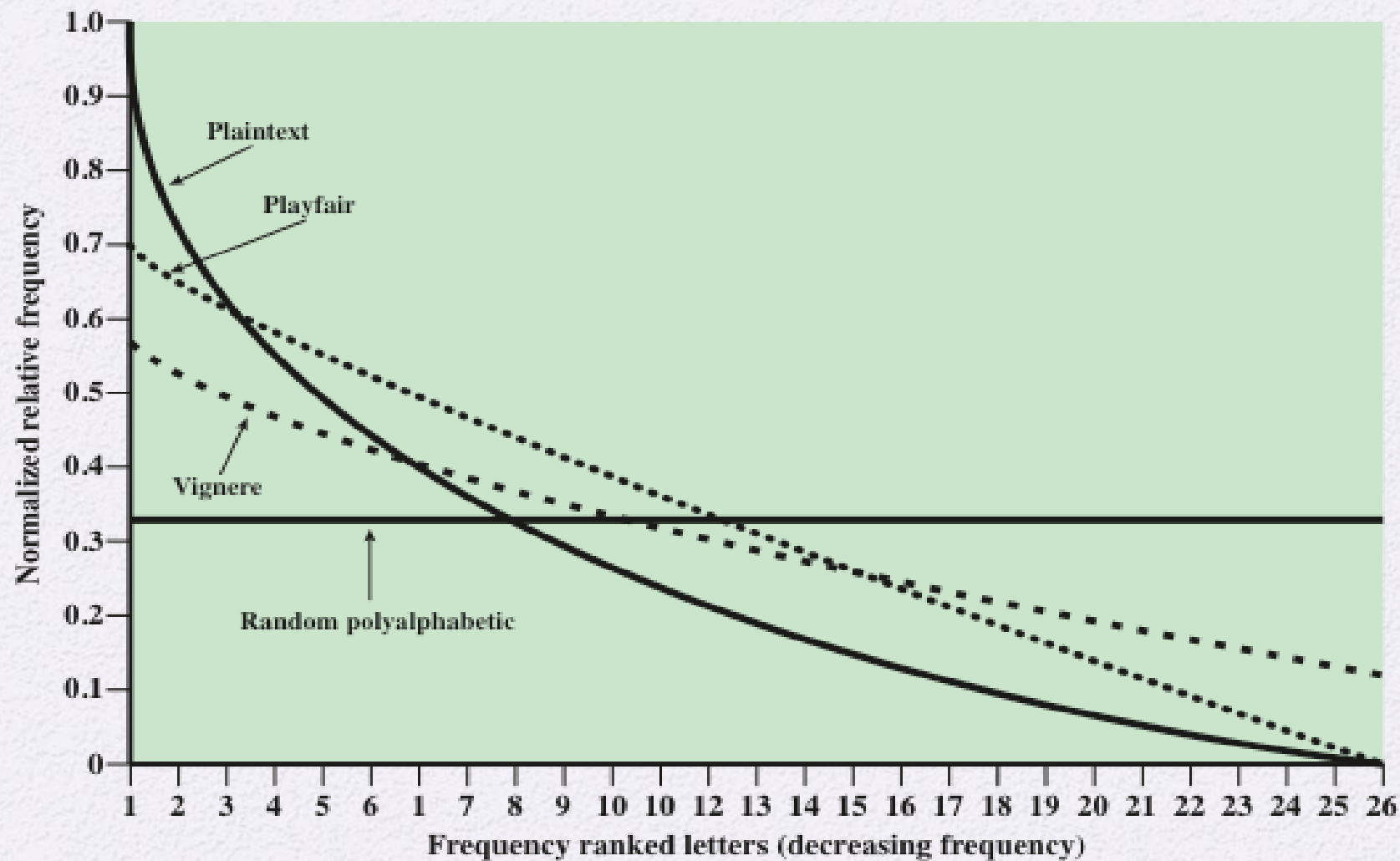


Figure 3.6 Relative Frequency of Occurrence of Letters

Hill Cipher

many to many

- By mathematician Lester Hill in 1929
- Completely hides single-letter frequencies
 - The use of a larger matrix hides more frequency information
 - A 3×3 Hill cipher hides not only single-letter but also two-letter frequency information
- Strong against a ciphertext-only attack,
- Easily broken with a known plaintext attack

Hill Cipher: method

- $K = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix}$
- $P = [p_1 \quad p_2 \quad p_3]$
- $C = PK \bmod 26$
- $P = CK^{-1} \bmod 26$
- Security: weak under the known plaintext attack
 - Given enough pairs of (P_i, C_i) , solve the linear equations

Polyalphabetic Ciphers

- Use a set of monoalphabetic substitutions
- A key determines which substitution is chosen for transformation

Vigenère Cipher

(different shift key every alphabet, key is counted from A)

- The simplest polyalphabetic substitution ciphers
- The set of monoalphabetic substitutions: 26
 - Caesar ciphers with shifts of 0 through 25
- Substitution X: $a \rightarrow X$

Vigenère: Example

- Key: as long as the message
 - the key is a repeating keyword
- For example,
 - keyword: deceptive
 - Message: we are discovered save yourself

key: **deceptive**deceptivedeceptive

plaintext: wearediscoveredsaveyourself

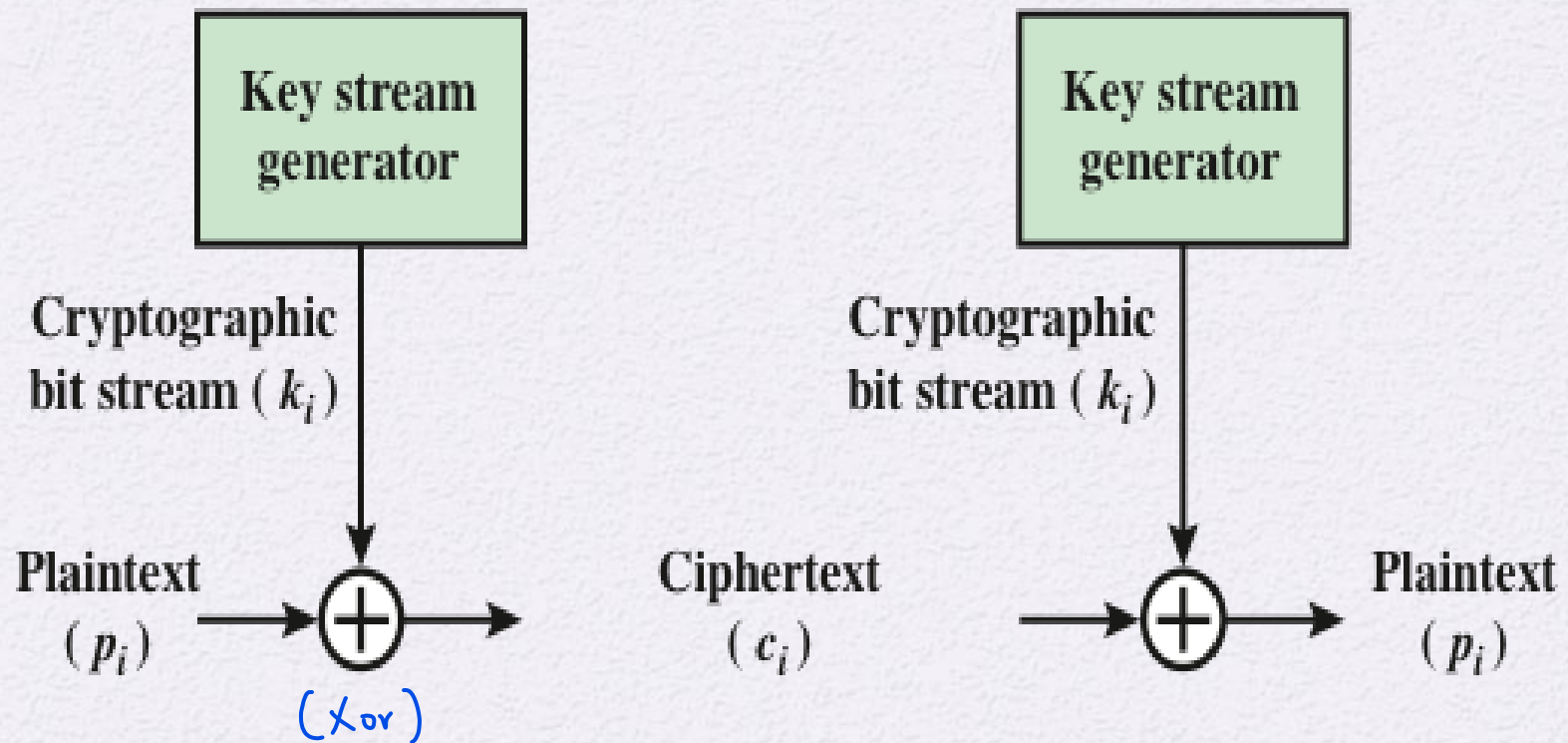
ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

a block \Rightarrow still can do frequency analysis

Vigenère: Autokey System

- A keyword is concatenated with the plaintext itself to provide a running key
- Example:
key: **deceptive**wearediscoveredsav
plaintext: wearediscoveredsaveyourself
ciphertext: ZICVTWQNGKZEIIGASXSTSLVWLA
- Still vulnerable to cryptanalysis
 - the key and the plaintext share the same frequency distribution of letters,
 - a statistical analysis can be applied

Vernam Cipher



One-Time Pad (OTP)

- By an Army Signal Corp officer, Joseph Mauborgne
- Improvement to Vernam
 - Key is truly random and as long as the message
 - Key is used only once
- Scheme is unbreakable
 - perfectly secure, unconditionally secure
 - ciphertext is random, no statistical relationship to the plaintext

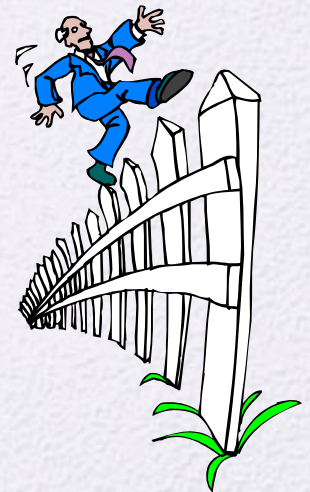
One-time pad: difficulties

- Two fundamental difficulties
 - Hard to produce long truly random keys
 - Key distribution problem: sender and receiver are hard to agree on a key, which is used only once
- The one-time pad is of limited utility
 - Useful primarily for low-bandwidth channels requiring very high security

ex. 飛機と塔台通訊

Rail Fence Cipher

- A simple transposition cipher
- Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows
- Example: rail fence with depth 2
 - Plaintext: “meet me after the toga party”
 - Encryption:
mematrhtgpry
etefeteoaat
 - Ciphertext: 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: TTNA APTM TSUO AODW COIX KNLY PETZ

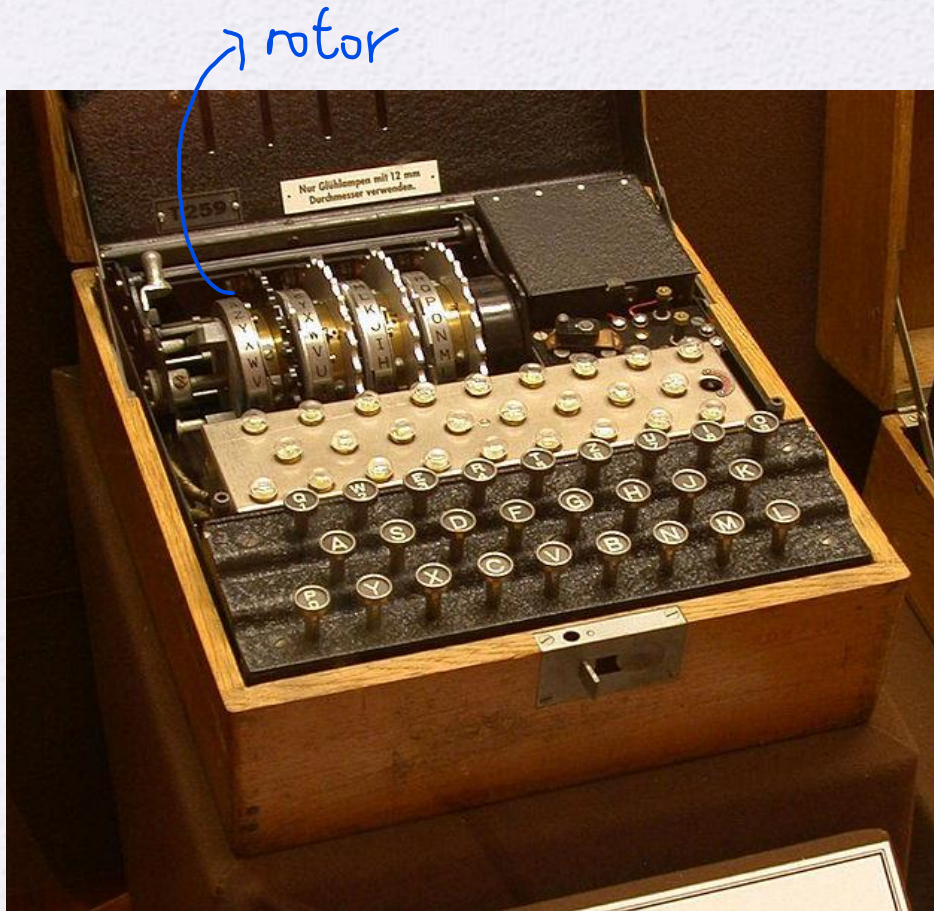
Enigma

- A polyalphabetic cipher with intricate design for practical use
- A rotor is a substitution
- One stroke of input rotates one position in the first cylinder
 - Polyalphabetic cipher with period 26
- One complete rotation of the first cylinder → one position in the second cylinder
- Three motors: $26 \times 26 \times 26 = 17576$ substitution possibilities for an alphabet



Viewed as a block

Enigma



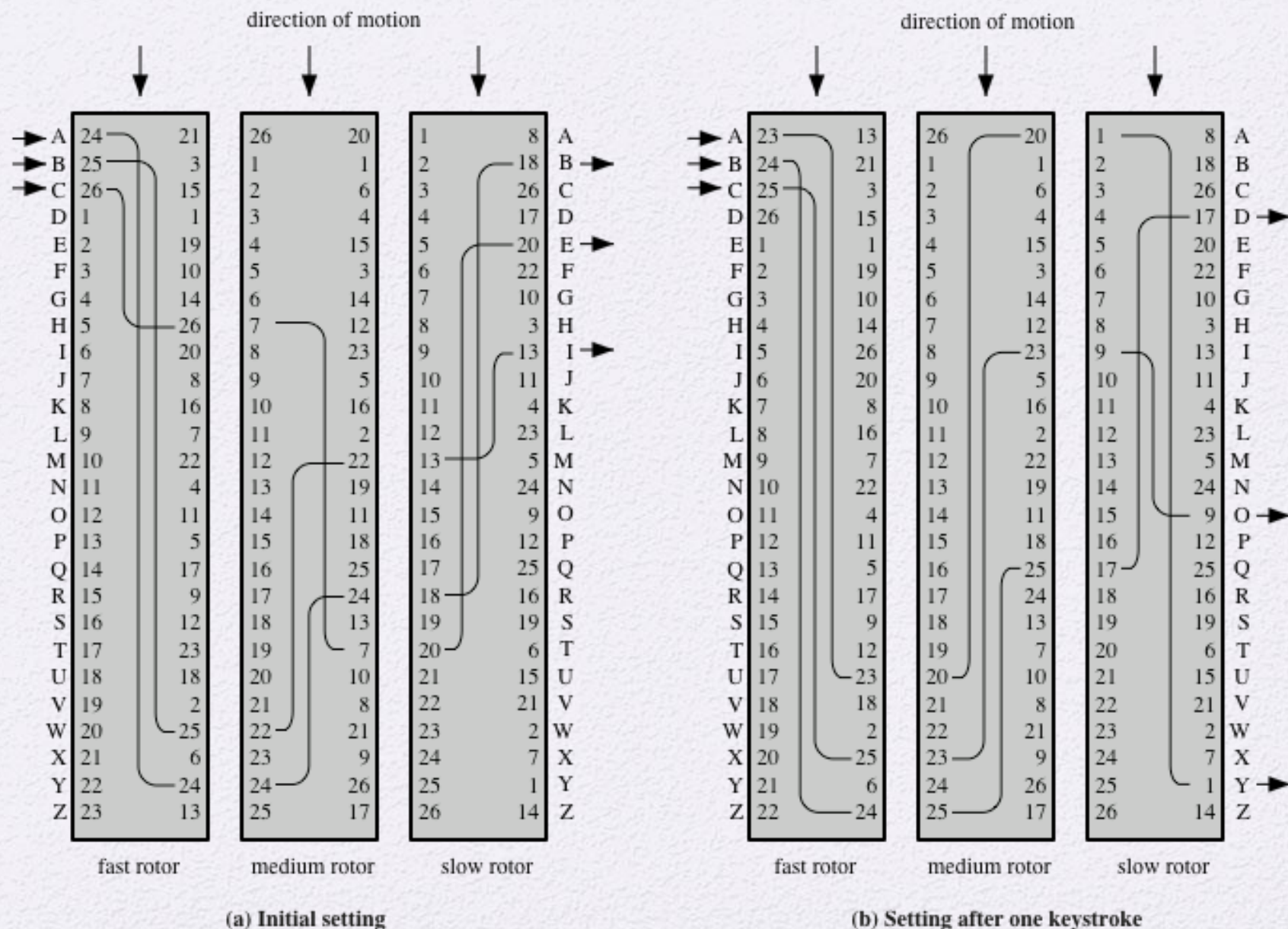
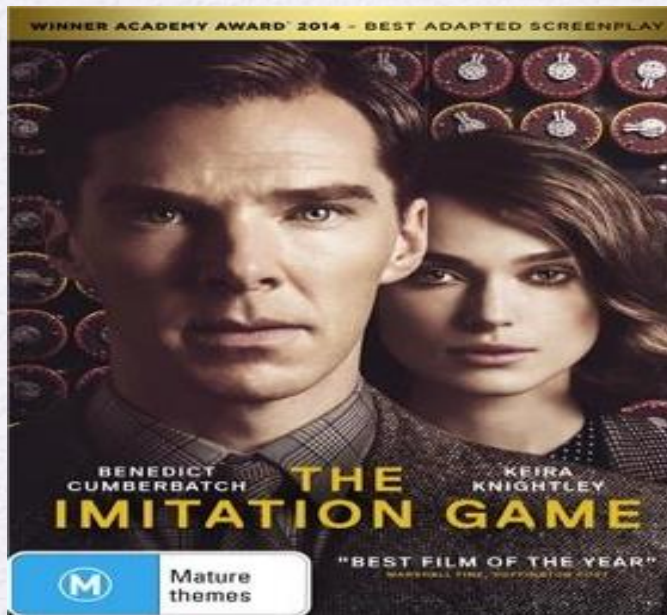


Figure 3.8 Three-Rotor Machine With Wiring Represented by Numbered Contacts

Enigma

- German cipher in WWI
- It was broken by The Allies
- The team was led by Allen Turing



Steganography

藏密詩/文

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,


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

What information is carried in this letter?

Hide data in images

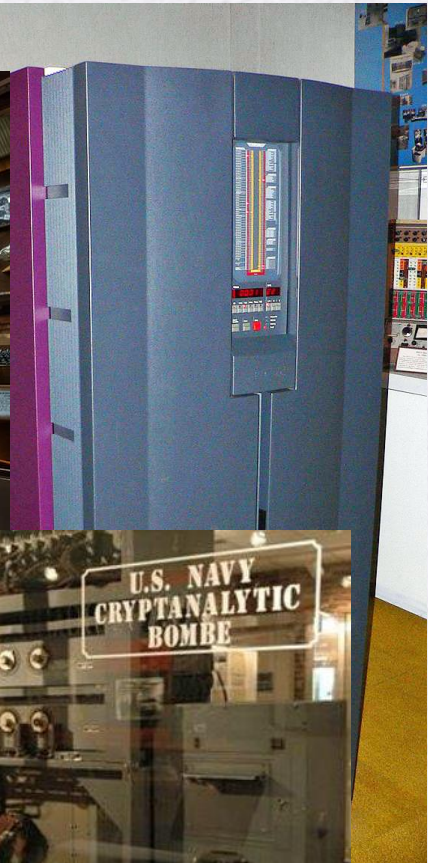


Digital Steganography
LSB IN IMAGES



144	141	81
10010000	10001101	01010001
Hidden message: 101001...		
145	140	81
1001000 1	1000110 0	0101000 1
146	142	81
100100 10	100011 10	010100 01

National Cryptologic Museum, US



Summary

- Symmetric Cipher Model
 - Cryptography
 - Attacks
- Transposition techniques
 - Rail Fence cipher
 - Row transposition cipher
- Enigma
 - Rotor machines
- Substitution techniques
 - Caesar cipher
 - Monoalphabetic ciphers
 - Playfair cipher
 - Hill cipher
 - Polyalphabetic ciphers
 - One-time pad
- Steganography