

Cryptography

Contents

- 1) Basic Terminology of cryptography
- 2) History of cryptography
- 3) Symmetric Cipher
- 4) Asymmetric Cipher
- 5) Hashing algorithms

1. Basic Terminology

Basic Terminology

- **Plaintext:** The original message
- **Ciphertext:** the crypted message
- **Encryption:** the process of converting plaintext into ciphertext



- **Decryption:** the process of recovering ciphertext into plaintext

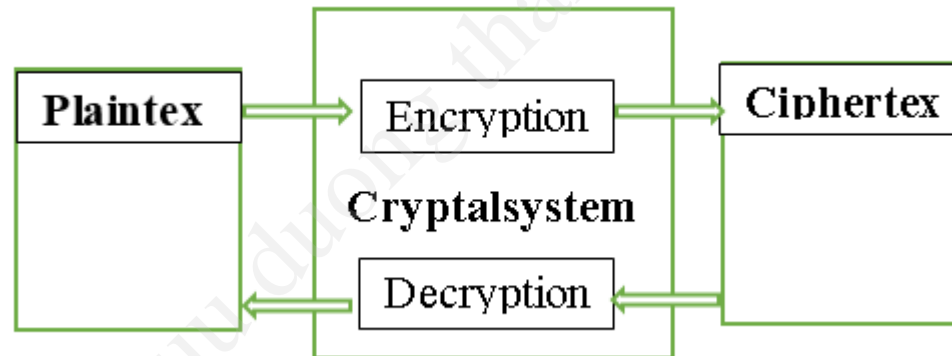


- **Cipher:** is an algorithm to encrypt or decrypt information.

Basic Terminology

- **Cryptosystem:** The algorithms, or ciphers, used to encrypt and decrypt data

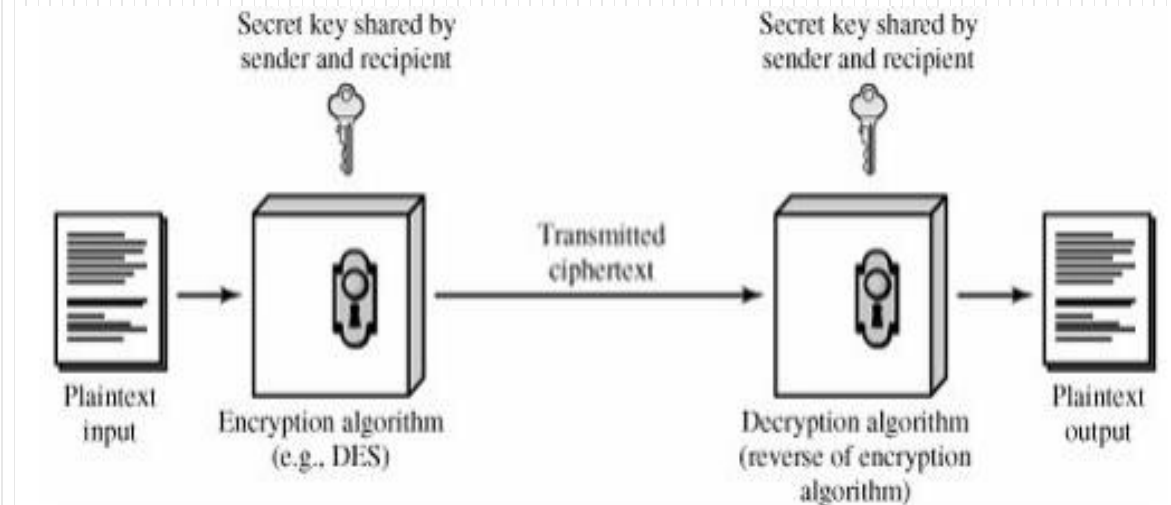
Cryptosystem = encryption + decryption algorithms.



- **Key:** info used in cipher known only to sender/receiver

Cryptology

- **Cryptography:** is the Science of Writing in Secret Code
- **Cryptanalysis:** science of studying attacks against cryptographic systems
- **Cryptology = Cryptography + Cryptanalysis**



Cryptography

Cryptographic systems are characterized along three independent dimensions

- Type of encryption operations used
 - Substitution: replacing each element of the plaintext with another element
 - Transposition: rearranging the order of the elements of the plaintext.
 - Product: using multiple stages of substitutions and transpositions

Cryptography

- Number of keys used:
 - Symmetric: single-key, private-key
 - Asymmetric: two-key, public-key
- way in which the plaintext is processed
 - Block cipher: processes the input one block of elements at a time
 - Stream cipher: processes the input elements continuously

Cryptanalysis

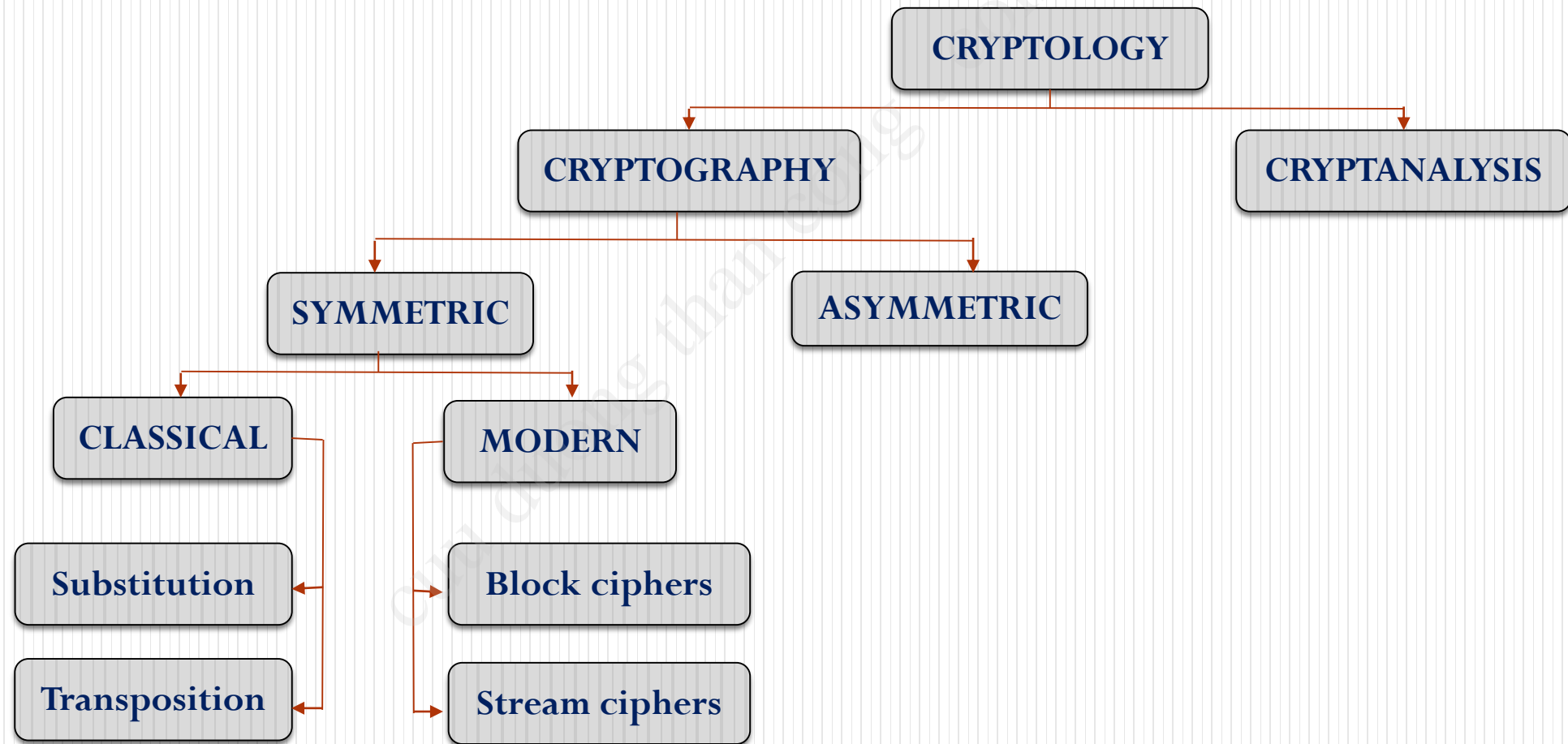
- **Objective:** to recover the key in use rather than simply to recover the plaintext of a single ciphertext.
- Two general approaches:
 - Brute-force attack: try every key to decipher the ciphertext
 - Cryptanalysis attack: exploit the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used

Cryptanalysis

- Brute-force attack: On average, half of all possible keys must be tried to achieve success.

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/ μ s	Time Required at 10^6 Decryptions/ μ s
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

Cryptology

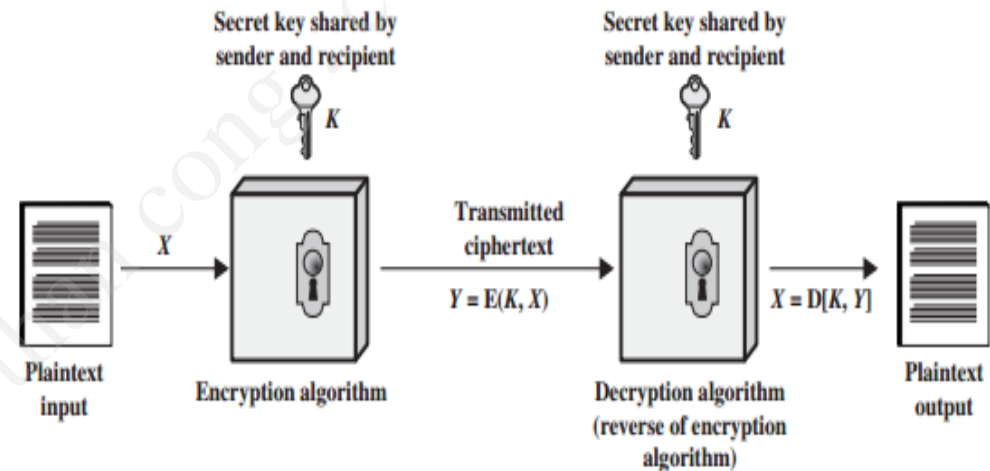


2. Symmetric Ciphers

- A. Classical Encryption
- B. Modern Encryption

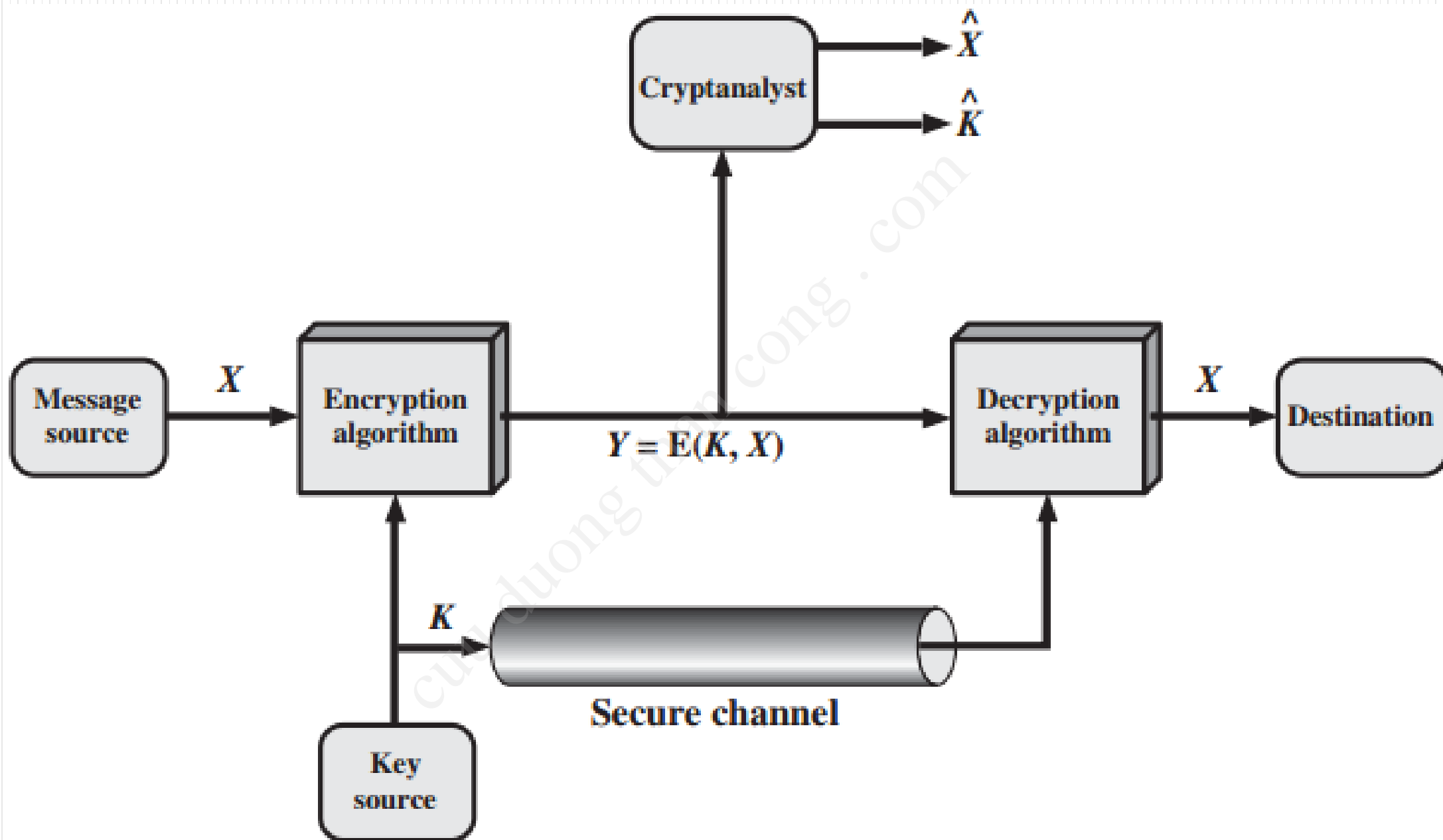
SYMMETRIC CIPHER MODEL

- Plaintext
- Encryption algorithm
- Secret key
- Ciphertext
- Decryption algorithm



Requirements

- Two requirements for secure use of symmetric encryption:
 - strong encryption algorithm
 - secret key know only to sender/receiver
- Mathematically have
 - $Y=E(K,X)$
 - $X=D(K,Y)$
- assume encryption algorithm is known
- implies a secure channel to distribute key



A. Classical encryption

- Caesar Cipher
- Monoalphabetic Ciphers
- Playfair Cipher
- Hill Cipher
- Polyalphabetic Ciphers
- One-Time Pad

Substitution Techniques

A. Classical encryption (Cont.)

- Transposition Techniques
- Steganography

Substitution Techniques

a) Caesar Cipher

- Invented by Julius Caesar.
- Each letter is replaced by the letter K positions further down the alphabet.

Example:

- Plaintext: **meet me after the toga party**
- Key: $k=3$

plain:	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
cipher:	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

- Ciphertext: **PHHW PH DIWHU WKH WRJD SDUWB**

a) Caesar Cipher

- Mathematically, map letter to numbers:

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

- $C = E(P, k) = (P + k) \bmod 26$
- $P = D(C, k) = (C - k) \bmod 26$

C: Ciphertext letter

P: Plaintext letter

K: Key [1-25]

Plaintext = “Go to the canteen after class”, $k = 4$

Ciphertext = ???

Cryptanalysis of Caesar Cipher

- Key space: $\{1, \dots, 25\}$
- Vulnerable to brute-force attacks
- Example: Break ciphertext “UNOU YZGZK”

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	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	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	zkbdj
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

b) Monoalphabetic Cipher

- A **permutation** of a finite set of elements is an ordered sequence of all the elements of , 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

There are $n!$ permutations of a set of n elements

- Substitution characters are a random permutation of the 26 letters of the alphabet

Monoalphabetic Cipher

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

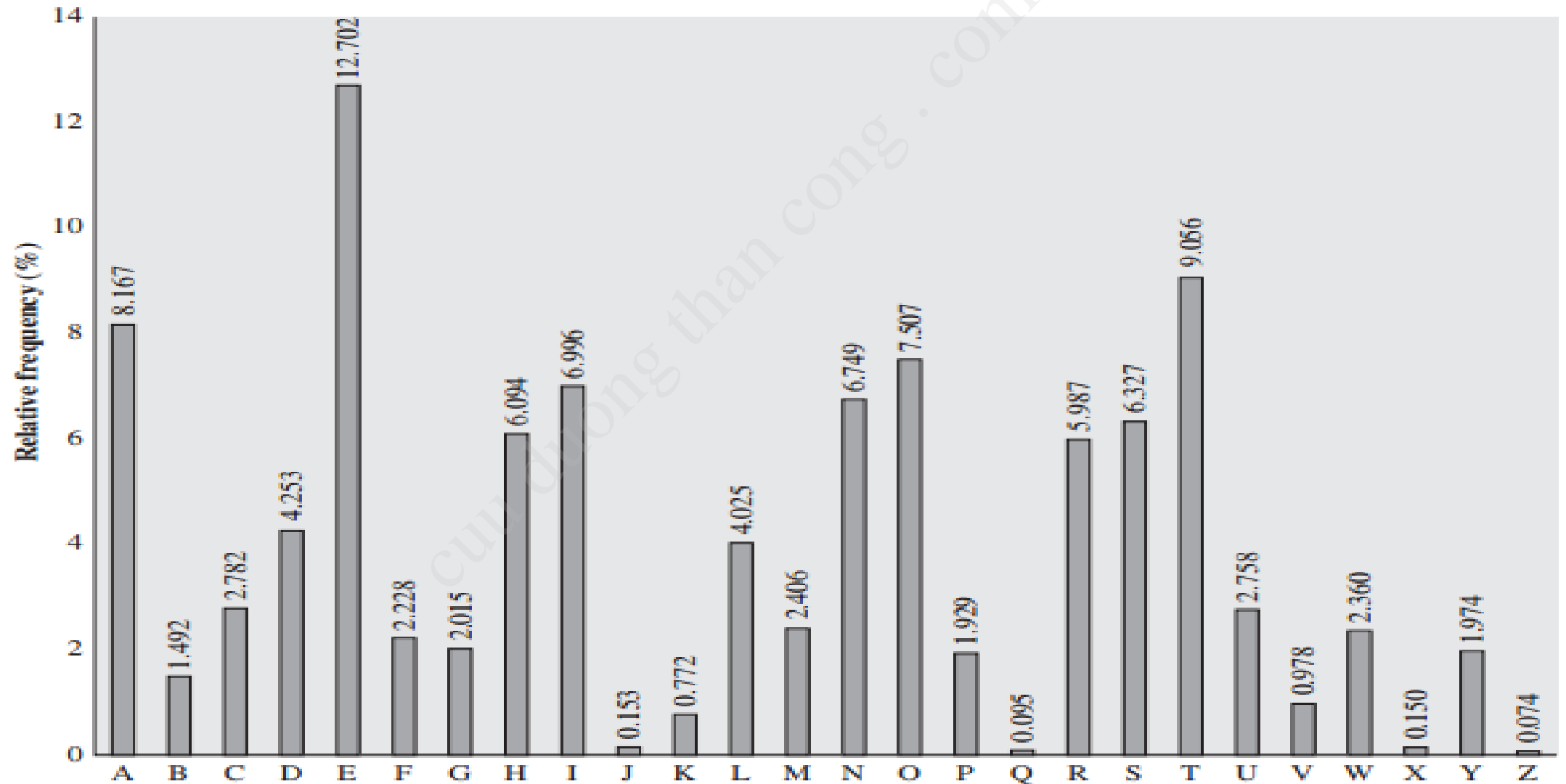
Plaintext: “**meet me after the toga party**”

Ciphertext: ???

Monoalphabetic Cipher Security

- 26! Key
- It is secure against brute-force attacks.
- But not secure against some cryptanalytic attacks
- Problem is language characteristics.

Relative Frequency of Letters in English Text



Statistics for double & triple letters

Single Letter	Double Letter	Triple Letter
E	TH	THE
T	HE	AND
R	IN	TIO
N	ER	ATI
I	RE	FOR
O	ON	THA
A	AN	TER
S	EN	RES

Cryptanalysis of Monoalphabetic

- Example: The ciphertext to be solved is

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ

VUEPHZHMZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

Cryptanalysis of Monoalphabetic

- The relative frequencies of the letters in the ciphertext (in percentages) are as follows:

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				

- Guess {P, Z} – {E,T}
- {S, U, O, M, H} – {a, h, i, n, o, r, s}
- {A, B, G, Y, I, J }– {b, j, k, q, v, x, z}

Cryptanalysis of Monoalphabetic

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ

t e e t e a t t e e

VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

e t t t e e e t t

EPYEPOPDZSZUFPOMBZWPFPUPZHMDJUDTMOHMQ

e e e t t e t e t

- Double letters: ZQ-1, ZP-1, ZW-3, ZO-2, ZH-2, ZS-2, ZU-2

=> Z->t; W->h

Cryptanalysis of Monoalphabetic

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

- Next, notice the sequence ZWSZ in the first line. th_t.

S->a

c) Playfair Cipher

- Invented by Charles Wheastone in 1854, but named after his friend Baron Playfair.
- Multiple-letter encryption cipher
- Security is much improved over the simple monoalphabetic cipher

Playfair Key Matrix

- Use a 5x5 matrix
- Fill in letter of the key (without duplicating letters)
- Fill the rest of matrix with other letters.

Example: key = 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

Plaintext is encrypted two letters at a time

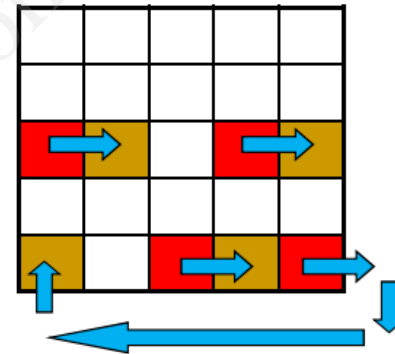
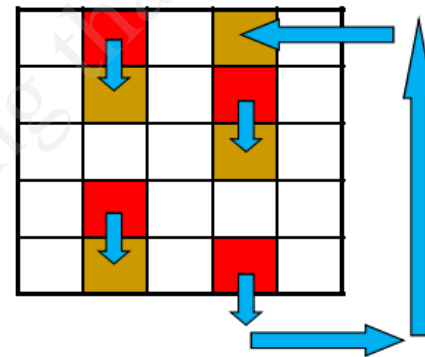
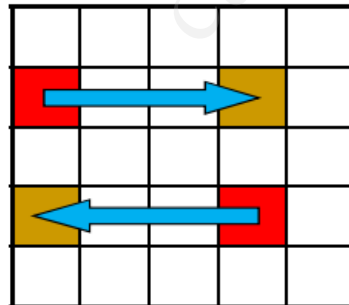
- Break the plaintext into pairs of two consecutive letters
- If a pair is a repeated letter, insert filler like 'x'
- If both letters fall in the same row, replace each with the letter to its right (circularly)
- If both letters fall in the same column, replace each with the letter below it (circularly).
- Otherwise, each letter is replaced by the letter in the same row but in the column of the other letter of the pair

Playfair Cipher

Example:

- Plaintext: **balloon**

=> **ba lx lo on**



Playfair Cipher

Example:

- Plaintext: **“hide the gold in the tree stump”**
- Key: **“playfair example”**
- Ciphertext ?

Security of playfair cipher

- Security much improved over monoalphabetic
 - There are $26 \times 26 = 676$ diagrams
- Needs a 676 entry diagram frequency table to analyse and correspondingly more cipher text
- Widely used for many years
- Can be broken, give a few hundred letters
 - Still has much of plaintext structure

d) Hill Cipher

- Invented by Lester Hill in 1929
- Multi-letter cipher



- Linear algebra: we are concerned with matrix arithmetic modulo 26

The inverse M^{-1} of a square matrix $M(m \times m)$:

$$MM^{-1} = M^{-1}M = I_m$$

Hill Cipher

$$\mathbf{A} = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix} \quad \mathbf{A}^{-1} \bmod 26 = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$$

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

Hill Cipher

- The encryption algorithm takes m successive plaintext letters and substitutes for them m ciphertext letters.
- Each character is assigned a numerical value: (a =0, b =1, c, ... z =25)

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: $C = PK \bmod 26$
- Decryption: $P = K^{-1}C \bmod 26$

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \bmod 26$$

Hill Cipher

- Example:

Plaintext: **paymoremoney**

Key:

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

The first three letters of the plaintext are represented by the vector (15, 0, 24)

Hill Cipher

- **Encryption:** $C = PK \bmod 26$

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} \mathbf{15} \\ 0 \\ 24 \end{bmatrix} \bmod 26 = \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} = \text{LNS}$$

- The ciphertext for the entire plaintext is **LNS???**

Hill Cipher

- **Decryption**

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

$$K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

Vì:

$$\begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} = \begin{bmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{bmatrix} \mod 26 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Khi đó bảng giải mã là: $K^{-1}C \mod 26 = K^{-1}KP \mod 26 = P$

e) Polyalphabetic Ciphers

- Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message.
- The features in common:
 - A set of related monoalphabetic substitution rules is used
 - A key determines which particular rule is chosen for a given transformation

Vigenere Cipher

- Simplest polyalphabetic substitution cipher.

- Plaintext: $P = p_0, p_1, p_2, \dots, p_{n-1}$

- Key consisting of the sequence of letters

$$K = k_0, k_1, k_2, \dots, k_{m-1}; \quad m < n$$

- ciphertext letters

$$C = C_0, C_1, C_2, \dots, C_{n-1}$$

Vigenere Cipher

$$\begin{aligned} C &= C_0, C_1, C_2, \dots, C_{n-1} = E(K, P) = E[(k_0, k_1, k_2, \dots, k_{m-1}), (p_0, p_1, p_2, \dots, p_{n-1})] \\ &= (p_0 + k_0) \bmod 26, (p_1 + k_1) \bmod 26, \dots, (p_{m-1} + k_{m-1}) \bmod 26, \\ &\quad (p_m + k_0) \bmod 26, (p_{m+1} + k_1) \bmod 26, \dots, (p_{2m-1} + k_{m-1}) \bmod 26, \dots \end{aligned}$$

- Encryption:

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

- Decryption

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

Vigenere Cipher- Example:

Plaintext: *we are discovered save yourself*

Key: *deceptive*

plaintext: wearediscoveredsaveyourself
key: DECEPTIVEDECEPTIVEDECEPTIVE
ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

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

	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
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

f) One-Time Pad

- Joseph Mauborgne
- using a random key that is as long as the message.
- The key is to be used to encrypt and decrypt a single message, and then is Discarded.

Plaintext P:	wearediscoveredsaveyourself
Key K1 :	FHWYKLVKVKXCVDJSFSAPXZCVP
Ciphertext :	BLWPOODEMJFBTZNVNJQOJORGGU

One-Time Pad

Bản mã C :	BLWPOODEMJFBTZNJVJNJQOJORG
Khóa K_2 :	IESRLKBWJFCIFZUCJLZXAXAAPSY
Bản giải mã:	theydecidedtoattacktomorrow <i>(they decided to attack tomorrow)</i>
Bản mã C :	BLWPOODEMJFBTZNJVJNJQOJORG
Khóa K_3 :	FHAHDDRAIQFIASJGJWQSVVBJAZB
Bản giải mã:	wewillmeetatthepartytonight <i>(we will meet at the party tonight)</i>

TRANSPOSITION TECHNIQUES

Transposition Techniques

- Performing some sort of permutation on the plaintext letters.
- The simplest such cipher is the **rail fence** technique: plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- For Example: “meet me after the toga party”

M	E	M	A	T	R	H	T	G	P	R	Y	
	E	T	E	F	E	T		A	O	A	A	T

Encrypted message: MEMATRHTGPRYETEFETEOAAT

Transposition Techniques

- A more complex scheme is to 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

Steganography

Steganography

- Steganography is data hidden within data

Hidden message:

*Your package ready
Friday 21st room
three. Please destroy
this immediately*

3rd March

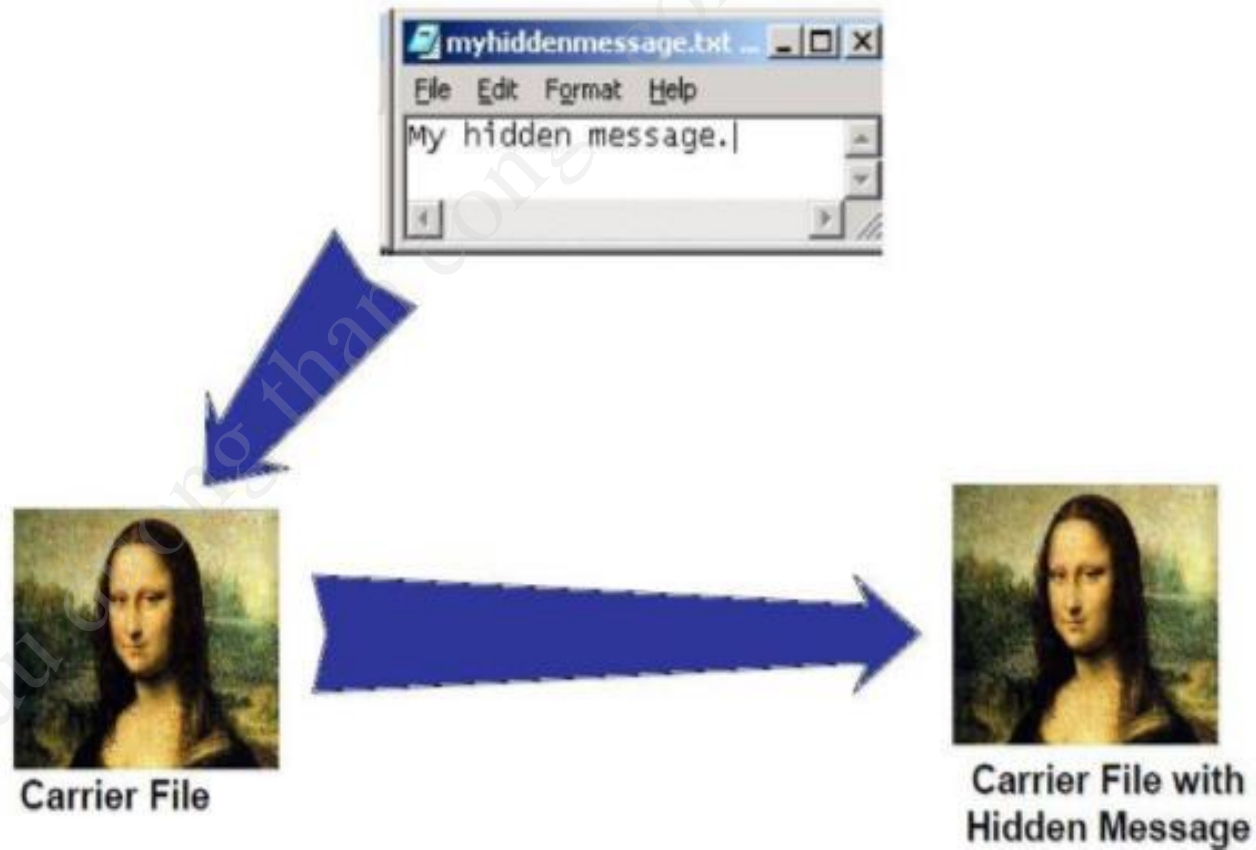
Dear George,

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 16t proposals destroy your basis O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

Steganography (cont.)

- **Tools:**
 - Image Steganograph
 - Xiao Steganography
 - Steghide
 - Crypture



Thanks