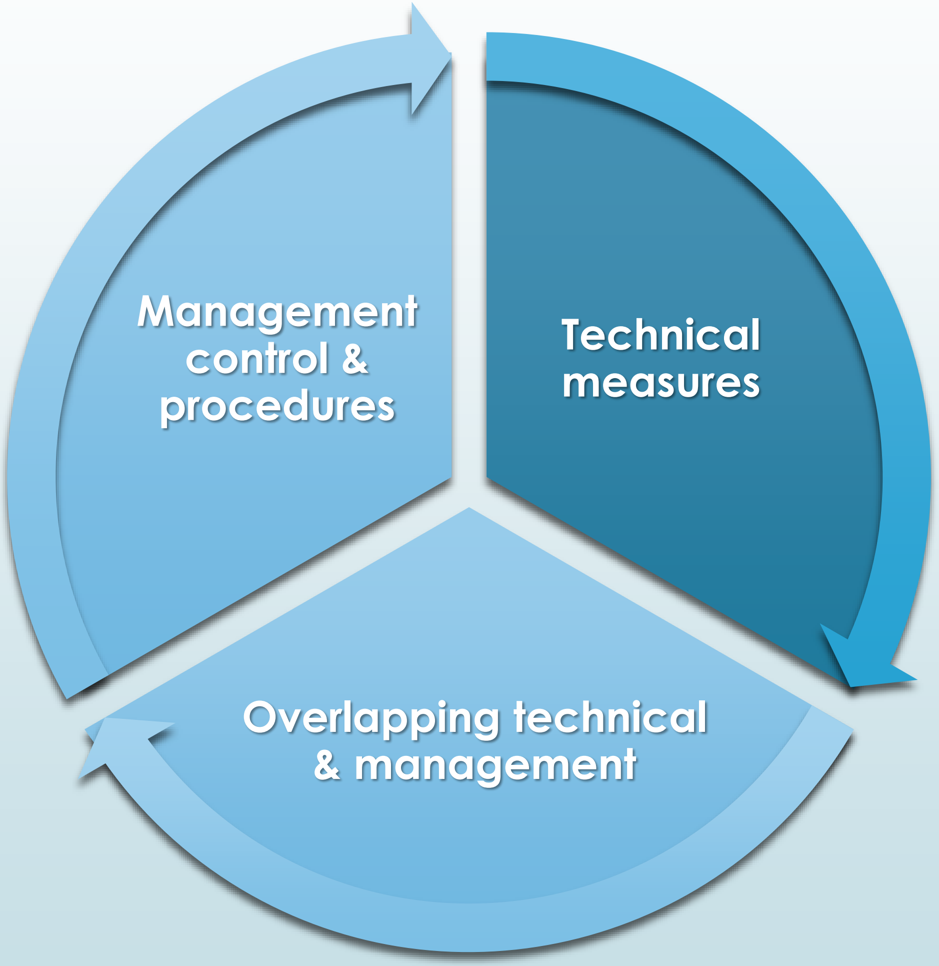
Computer security

Section 2

Eng : Asmaa Elsaid

Eng: Ahmed safar

Classification of countermeasures:


Management control & procedures
Technical measures
Overlapping technical & management

Technical measures

- Access control
- Identification & Authentication
- System & Communication Protection
- System & information integrity

Management control & procedures

- Awareness & training
- Audit & accountability
- Certification, accreditation, & security assessments
- Maintenance
- Planning
- Risk assessment

Overlapping technical & management

- ❖ Configuration management
- ❖ Incident response
- ❖ Media protection

Computer Security Strategy

- **Specification/Policy :**

- Security policy is a document that states in writing how a company plans to protect its (IT) assets.
- Security policy never finished, but is continuously updated as technology and employee requirements change.

❖ Implementation/Mechanisms :

- **Prevention**: An ideal security scheme is one in which no attack is successful.
- **Detection**: In a number of cases, absolute protection is not feasible, but it is practical to detect security attacks.
- **Response**: If security mechanisms detect an ongoing attack, the system may be able to respond in such a way as to halt the attack and prevent further damage.
- **Recovery**: An example of recovery is the use of backup systems, so that if data integrity is compromised, a prior, correct copy of the data can be reloaded.

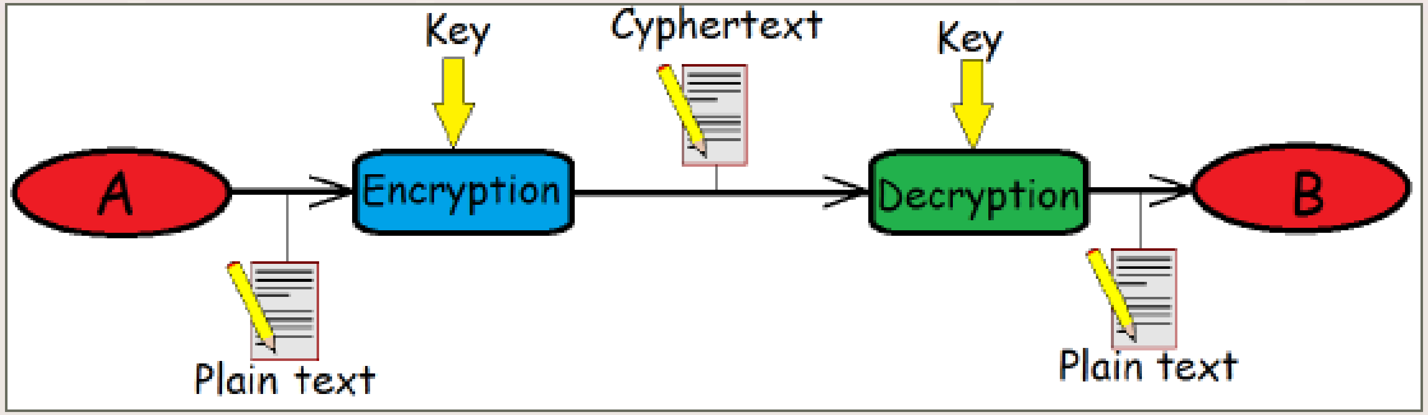
❖ Correctness/Assurance:

Assurance: is defined as the degree of confidence one has that the security measures, work as intended to protect the system and the information it processes. Assurance deals with the questions:

○ "Does the security system design meet its requirements?"

○ "Does the security system implementation meet its specifications?"

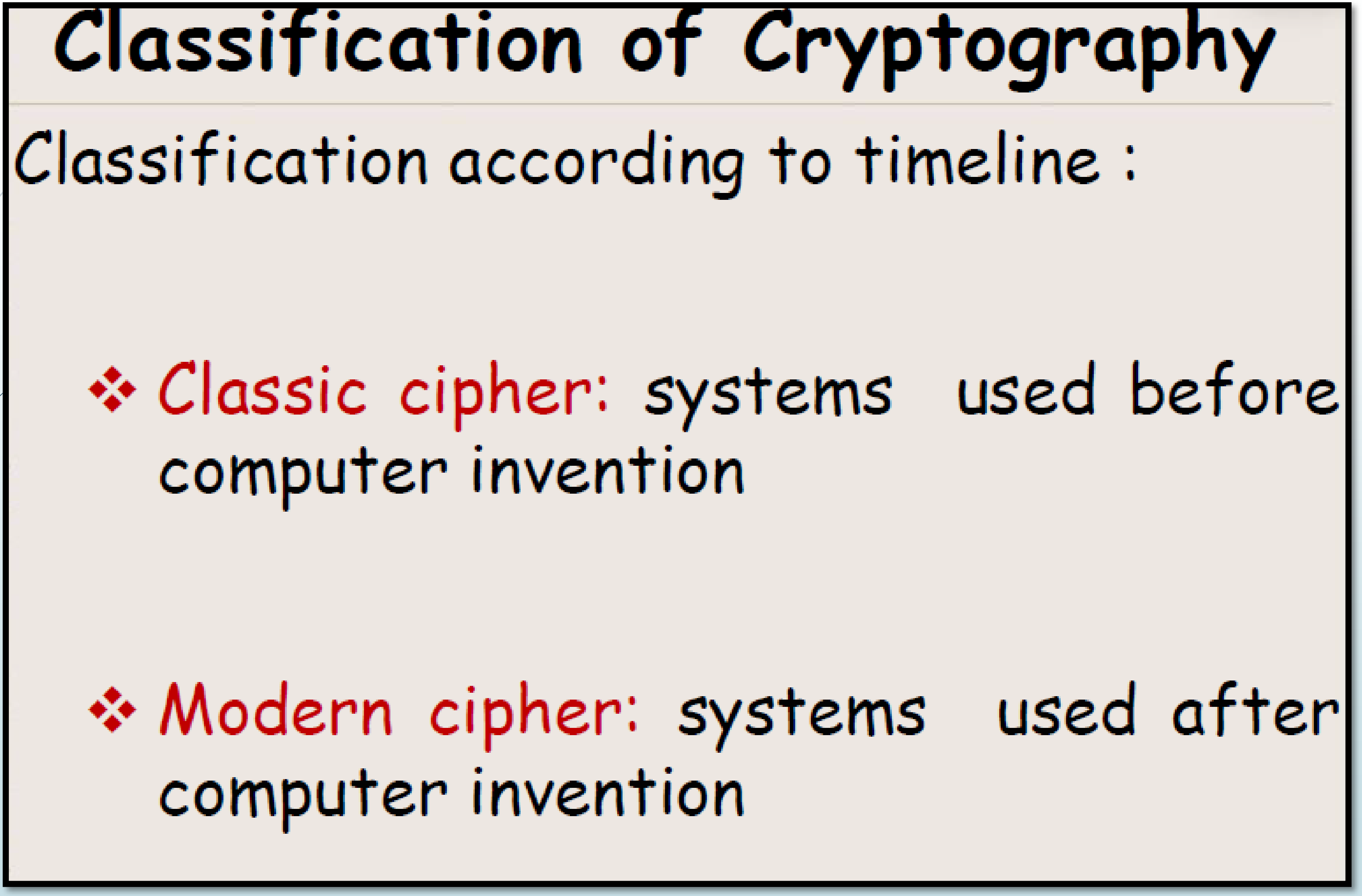
Definitions



Encryption: is the process of turning a clear-text message (Plaintext) into a meaningless and random sequence of bits (ciphertext). Alternate name (ciphering)

Decryption: is the process of turning ciphertext back into plaintext. Alternate names (decipher - decoding)

Cryptographic algorithm: is a mathematical function which uses plaintext as the input and produces ciphertext as the output and vice versa. (instructions for how to do the encryption/decryption)

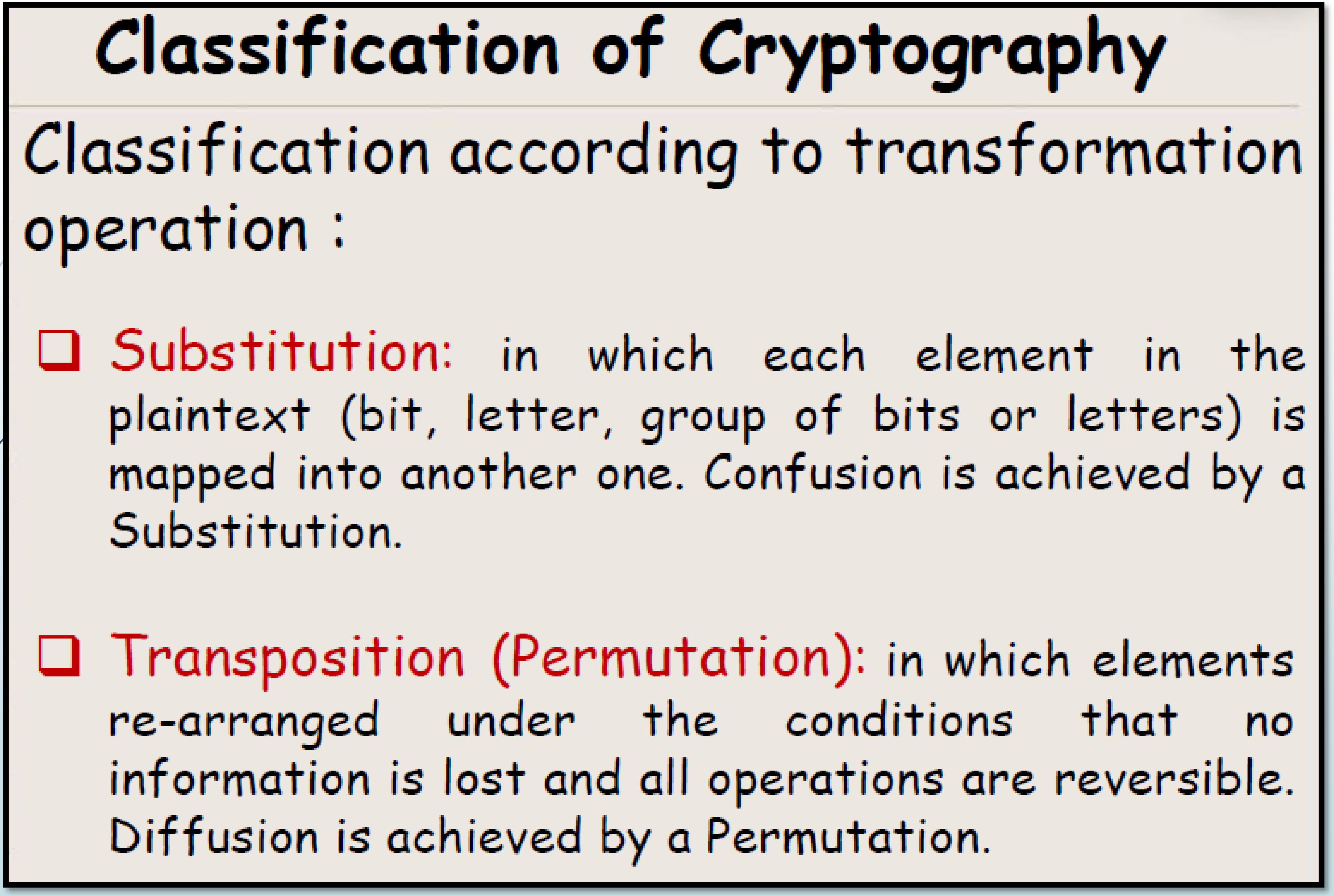


Classification of Cryptography

Classification according to timeline :

- ❖ Classic cipher: systems used before computer invention

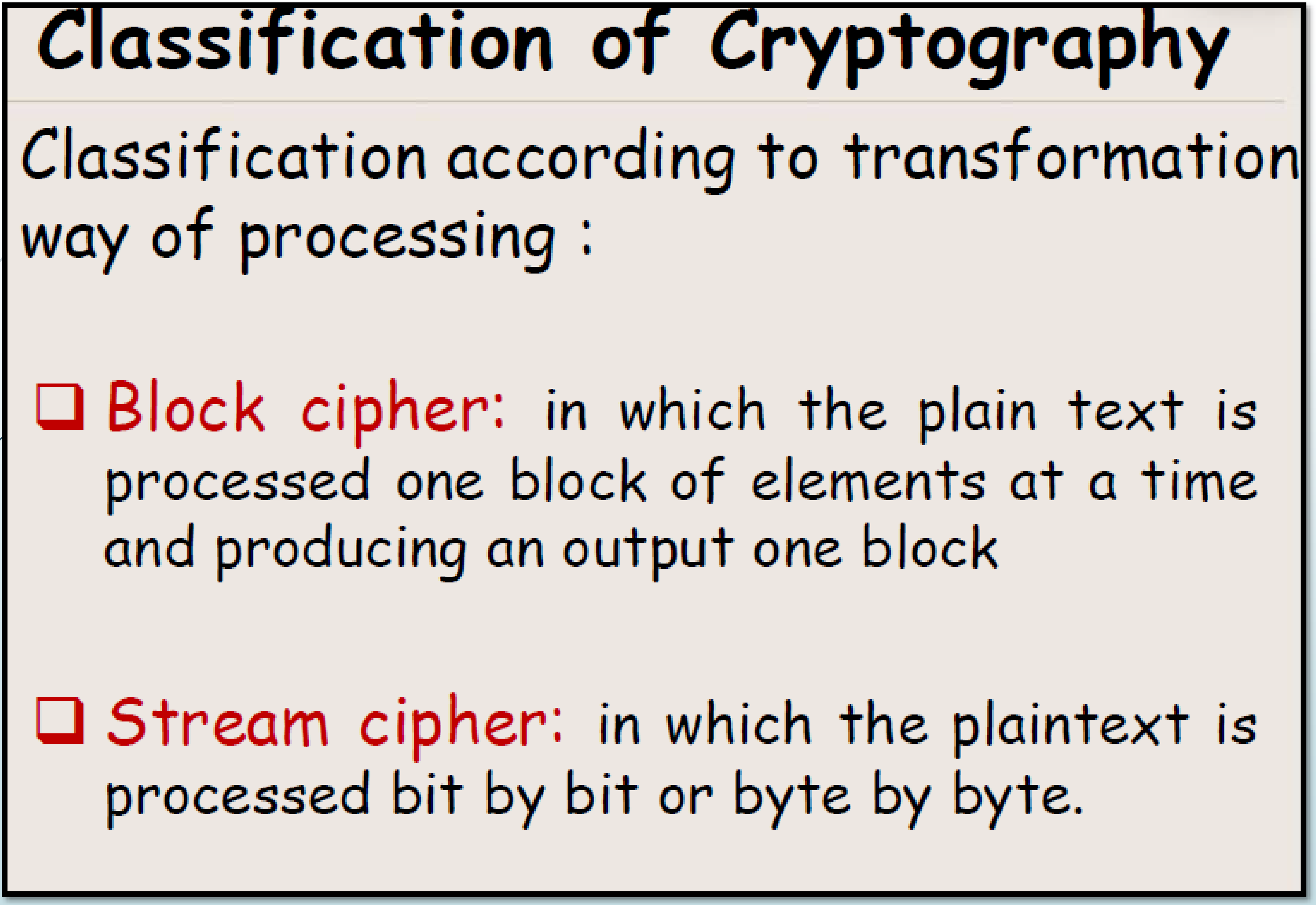
- ❖ Modern cipher: systems used after computer invention



Classification of Cryptography

Classification according to transformation operation :

- □ **Substitution:** in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another one. Confusion is achieved by a Substitution.
- □ **Transposition (Permutation):** in which elements re-arranged under the conditions that no information is lost and all operations are reversible. Diffusion is achieved by a Permutation.



Classification of Cryptography

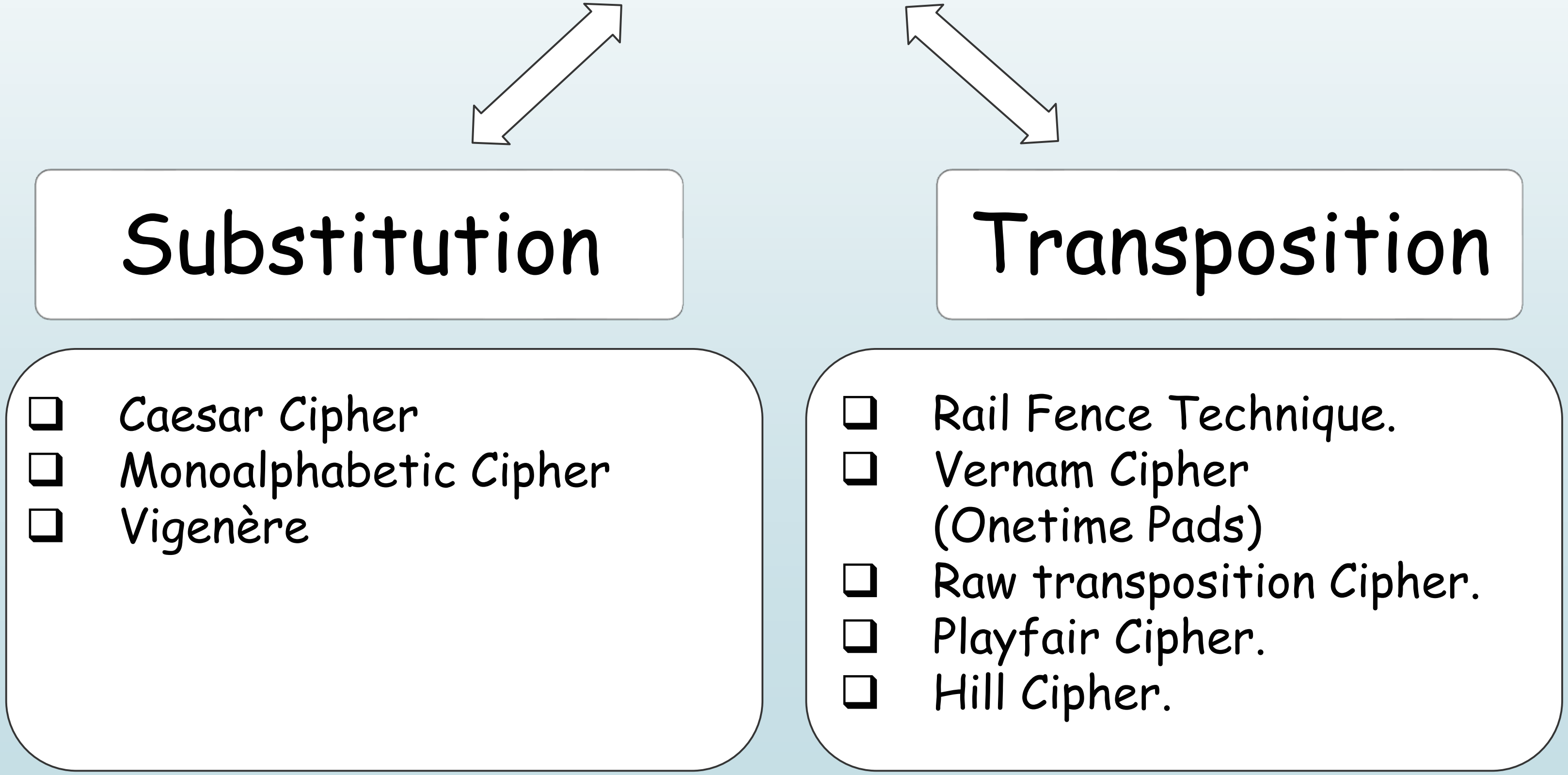
Classification according to transformation way of processing :

- □ Block cipher: in which the plain text is processed one block of elements at a time and producing an output one block

- □ Stream cipher: in which the plaintext is processed bit by bit or byte by byte.

Classification of Cryptography

Cryptography according to (transformation operation)



Substitution

❑ Caesar Cipher
❑ Monoalphabetic Cipher
❑ Vigenère

Transposition

❑ Rail Fence Technique.
❑ Vernam Cipher
(Onetime Pads)
❑ Raw transposition Cipher.
❑ Playfair Cipher.
❑ Hill Cipher.

Monoalphabetic Cipher

❑ each plaintext letter maps to a different random cipher text letter .

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

Example 1

if we wish to replace letters

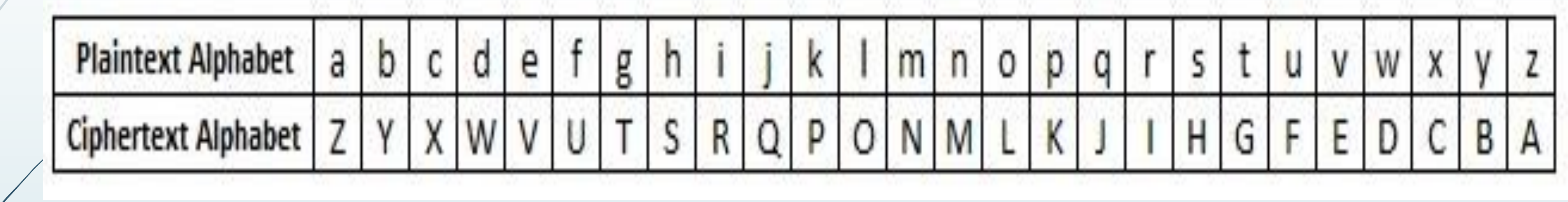
p	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c	d	k	v	q	f	i	b	j	w	p	e	s	c	x	h	t	m	y	a	u	o	l	r	g	z	n

Answer

Cipher text: **WI RF RWAJ UH YFTSDVF SFUUFYA**

Example 2

I study computer security



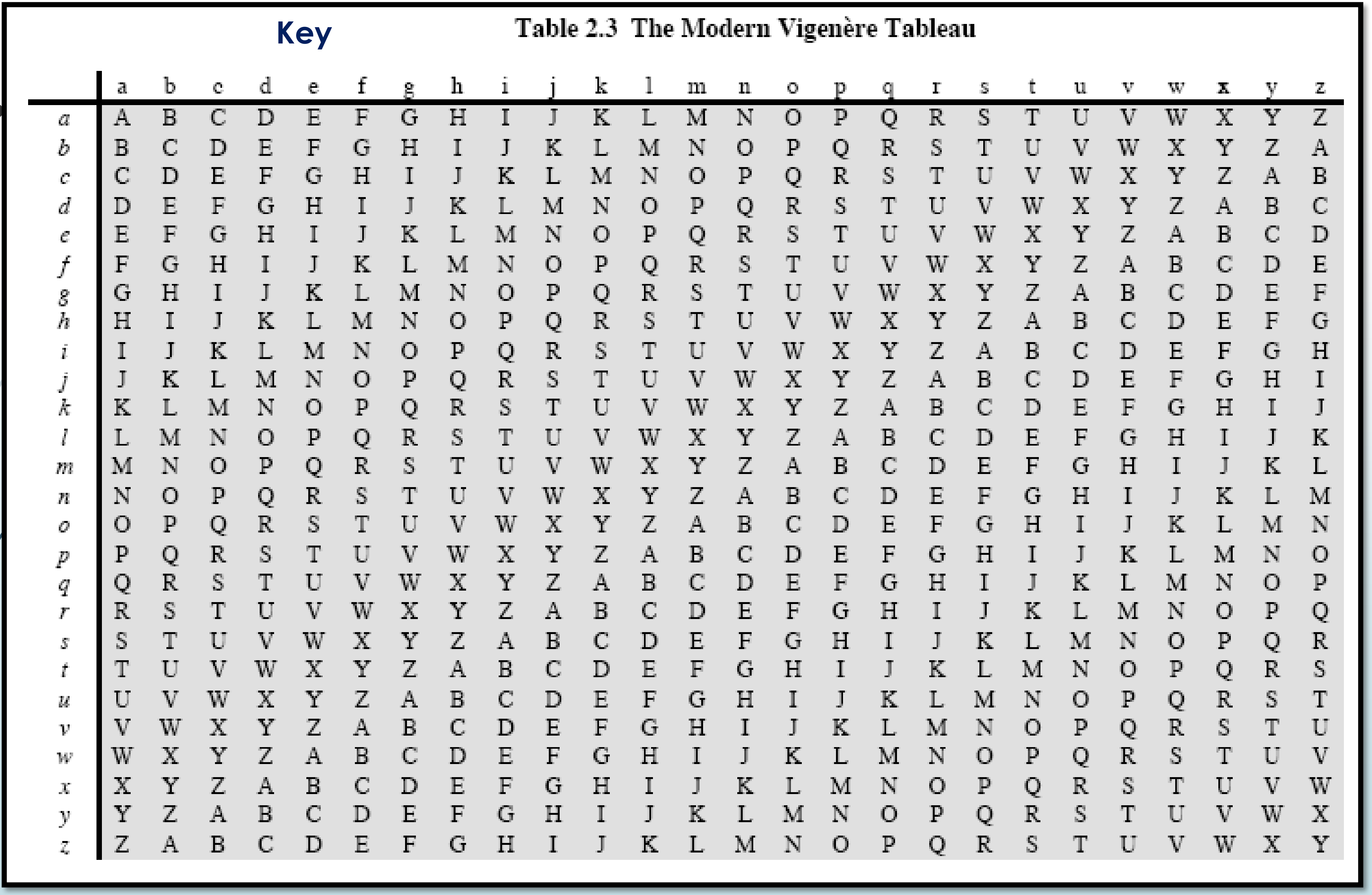
Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Answer

Cipher text： r hgfwb xlnkfgvi hvxfirgb

Vigenère Cipher

- ❑ Effectively multiple caesar ciphers
- ❑ Given a key letter X and a plain text Y, the cipher text letter is at inspection of the row labelled x and the column labelled y in this case the cipher text is V.



Key

Table 2.3 The Modern Vigenère Tableau

	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

Plaint text

Example 1

key: deceptive

plaintext: weare discovered save yourself

Answer

Plain text :wearediscoveredsaveyourself

key: :deceptivedeceptivedeceptive

Cipher text :ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Rail-Fence Cipher

❑ The plain text is written down a sequence of columns and then read off as a sequence of rows.

Example ciphering of “ meet me after the party”

Plaintext with Rail-Fence of depth 2:

m	e	m	a	t	r	h	p	r	y
e	t	e	f	e	t	e	a	t	-

The encrypted message is

mematrhpryetefeteat

Example 1

Plaint text : Computer Sciences

Key :3

Answer

c	P	e	c	n	s
o	U	r	i	c	
m	t	s	e	e	

Cipher text :cpecnsouricmtsee

Playfair Cipher

- one approach to improving security was to encrypt multiple letters
- a 5X5 matrix of letters based on a keyword
- fill in letters of keyword
- fill rest of matrix with other letters

eg. 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

Example 1

Plaint text : shrouk acadmy

Key :security

s	e	c	u	r
I / j	T	Y	A	B
D	F	G	H	K
L	M	N	O	P
Q	V	W	x	z

Answer

Plaint text	sh	ro	uk	ac	ad	my
Cipher text	ud	up	rh	yu	i/j h	nt

Example 2

Plaint text : The sky is blue

Key : keyword

K	E	Y	W	O
R	d	A	B	C
F	G	H	i/j	L
M	N	P	Q	S
T	U	V	X	z

Answer

Plaint text	Th	es	ky	is	bl	ue
Cipher text	Vf	on	ew	lq	ci	ed