

Cybersecurity Concepts

Prepared by Dr. Diaa Salama

FNT625
Classical Encryption Techniques (part 2)

Lecture 6





مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY

Cybersecurity Concepts

Lecture 6

FNT625

Classical Encryption Techniques(part 2)

Prepared by
Dr. Diao Salama

www.midocean.ae

PLEASE
BE QUIET



10



Lecture

06

Lets Start the sixth Lecture



Classical Encryption Techniques **Part 2**



Symmetric Encryption

Substitution Techniques

Caesar Cipher

Monoalphabetic Cipher

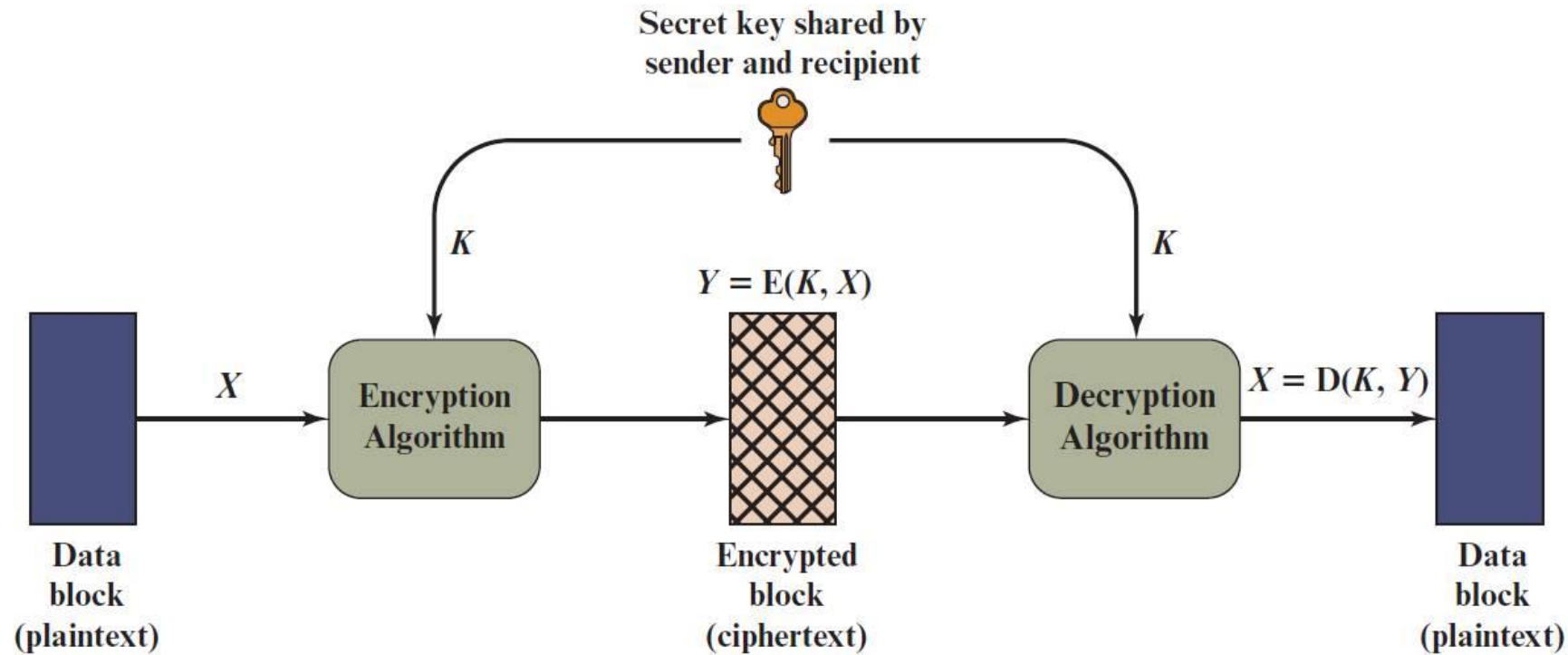
Symmetric Encryption

Substitution Techniques

Caesar Cipher

Monoalphabetic Cipher

Figure 3.1 Simplified Model of Symmetric Encryption



Definitions (1 of 2)

Lecture

06

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

Definitions (2 of 2)

- Cryptography
 - The area of study of the many schemes used for encryption
- Cryptographic system/cipher
 - A scheme
- Cryptanalysis
 - Techniques used for deciphering a message without any knowledge of the enciphering details
- Cryptology
 - The areas of cryptography and cryptanalysis

Symmetric Encryption

Substitution Techniques

Caesar Cipher

Monoalphabetic Cipher

Substitution Techniques

- ☐ Caesar Cipher
- ☐ Monoalphabetic Ciphers
- ☐ Playfair Cipher
- ☐ Hill Cipher
- ☐ Polyalphabetic Ciphers
- ☐ Vigenère Cipher
- ☐ Autokey Cipher
- ☐ Vernam Cipher

Symmetric Encryption

Substitution Techniques

Caesar Cipher

Monoalphabetic Cipher

Caesar Cipher Algorithm

Example: 1 Use the Caesar cipher to encrypt and decrypt the message "JAVATPOINT," and the key (shift) value of this message is 3.

Encryption

We apply encryption formulas by character, based on alphabetical order.

The formula of encryption is:

$$\text{En}(x) = (x + n) \bmod 26$$

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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 3.3 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	rfe	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	nsgrc	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	glzlx	znk	zumg	vqxze
24	rjyy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

Symmetric Encryption

Substitution Techniques

Caesar Cipher

Monoalphabetic Cipher

Lecture

06

monoalphabetic cipher

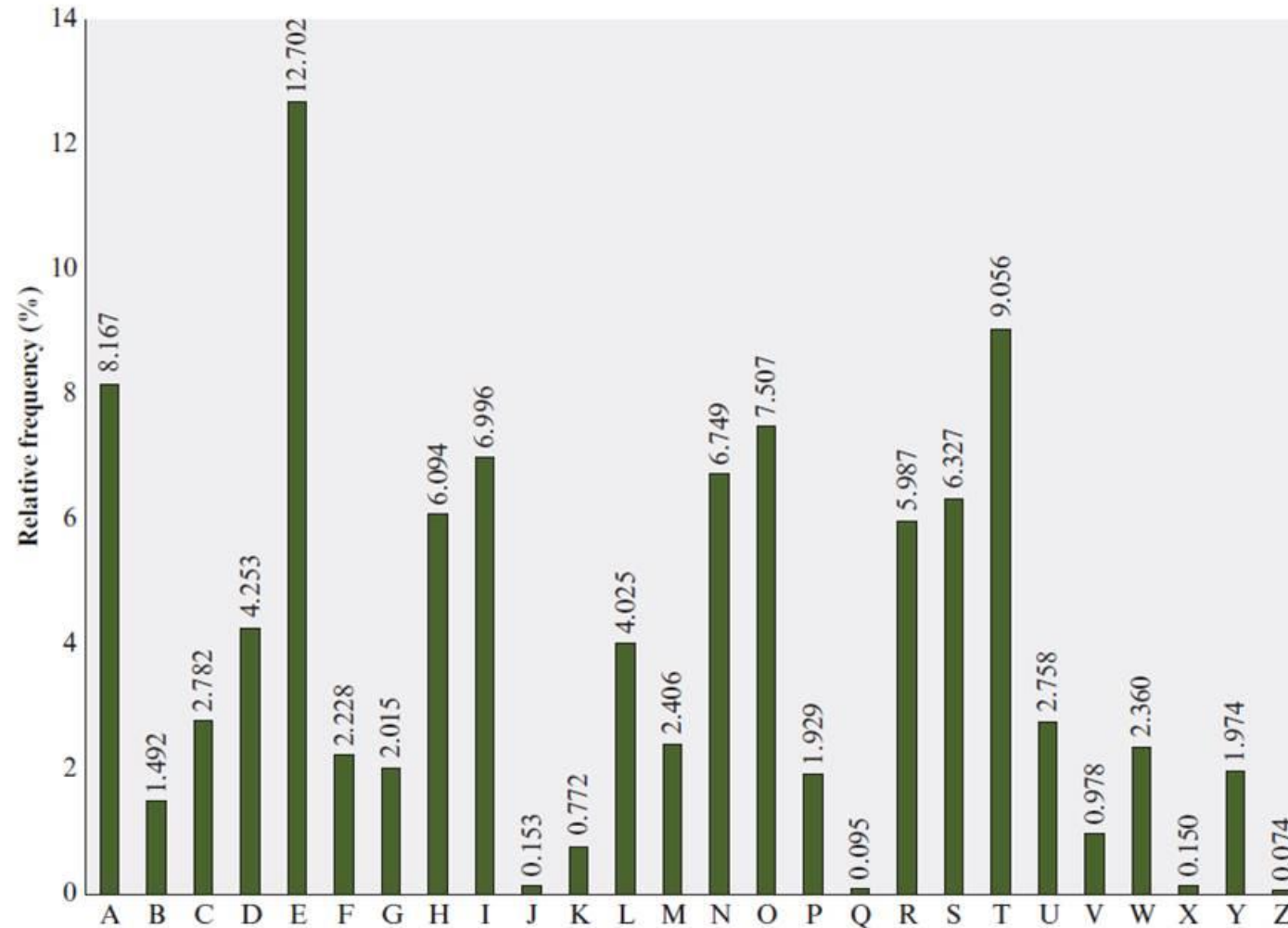
A mono-alphabetic cipher (aka simple substitution cipher) is a substitution cipher where each letter of the plain text is replaced with another letter of the alphabet. It uses a fixed key which consist of the 26 letters of a “shuffled alphabet”.

Plaintext : How Are you cipher text : ?????

<https://www.101computing.net/mono-alphabetic-substitution-cipher/>

Plain text alphabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
Cipher text alphabet (key):	M	U	A	L	V	O	Z	K	R	N	J	X	Q	D	F	S	H	P	E	B	C	T

Figure 3.5 Relative Frequency of Letters in English Text



Symmetric Encryption

Substitution Techniques

Caesar Cipher

Monoalphabetic Cipher

Playfair Cipher

Playfair cipher

- ❑ The Playfair system was invented by Charles Wheatstone, who first described it in 1854.
- ❑ Used by many countries during wartime
- ❑ The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword.

Playfair cipher

- ❑ In this case, the keyword is 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

Encryption and Decryption

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

- plaintext is encrypted two letters at a time
 1. if a pair is a repeated letter, insert filler like 'X'
 2. if both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
 3. if both letters fall in the same column, replace each with the letter below it (wrapping to top from bottom)
 4. otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair

Example

- Encrypting the message "Hide the gold in the tree stump":
- Using "playfair example" as the key

hi de th eg ol di nt he tr e^x es tu mp

P	L	A	Y	F ^A
I	R	E	X ^A	M ^{PLE A}
B	C	D ^{EF}	G	H ^{I=J}
K ^{LM}	N	O ^P	Q ^R	S
T	U	V	W ^{XY}	Z

Playfair cipher

- How to build 5x5 Matrix (assuming that I and J are interchangeable), the table becomes (omitted letters in red):

P	L	A	Y	F	A				
I	R	E	X	A	M	P	L	E	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			

Playfair cipher

□ P= **HI** DE TH EG OL DI NT HE TR **X** ES TU MP

1. The pair HI forms a rectangle, replace it with BM

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

HI

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

BM

Playfair cipher

❑ P=HI DE TH EG OL DI NT HE TR EX ES TU MP

2. The pair DE is in a column, replace it with OD

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

DE

Shape: Column
Rule: Pick Items Below Each Letter, Wrap to Top if Needed

OD

Playfair cipher

❑ P=HI DE **TH** EG OL DI NT HE TRE **X** ES TU MP

3. The pair TH forms a rectangle, replace it with ZB

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

TH

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

ZB

Playfair cipher

❑ P=HI DE TH **EG** OL DI NT HE TR **X** ES TU MP

4. The pair EG forms a rectangle, replace it with XD

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

EG

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

XD

Playfair cipher

❑ P=HI DE TH EG OL DI NT HE TR **EX** ES TU MP

10. The pair EX (X inserted to split EE) is in a row, replace it with XM

P L A Y F

I R **E** > **X** > **M**

B C D G H

K N O Q S

T U V W Z

EX

Shape: Row
Rule: Pick Items to Right of Each Letter, Wrap to Left if Needed

XM

Playfair cipher

- ❑ C= BM OD ZB XD NA BE KU DM UI XM MO UV IF
- ❑ the message "Hide the gold in the tree stump" becomes "BMODZ BXDNA BEKUD MUIXM MOUVI F"

Playfair cipher

- the message "Hide the gold in the tree stump" becomes "BMODZ BXDNA BEKUD MUIXM
MOUVI F"

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

Polyalphabetic Ciphers

Vigenère Cipher

Autokey Cipher

Vernam Cipher

Transposition Techniques

Rail Fence Cipher

Row Transposition Cipher

polyalphabetic cipher

- A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
- polyalphabetic cipher 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.

polyalphabetic cipher

☐ Assume

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

☐ Then We set these Rules:

polyalphabetic cipher

❑ Then We set Key as Rules:

- 1) Shift the first letter three position to the right
- 2) Shift the second letter five position to the right
- 3) Shift the third letter seven position to the right

❑ Given Plaintext = security

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

polyalphabetic cipher

❑ Given Plaintext = security

1) Divide Plaintext to three words

2) P= sec uri ty

3) C= VJJ XWP WD

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

polyalphabetic cipher Decryption

❑ Then We set Key as Rules: (reverse)

- 1) Shift the first letter three position to the **left**
- 2) Shift the second letter five position to the **left**
- 3) Shift the third letter seven position to the **left**

❑ Given Ciphertext = VJJXWPWD

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

polyalphabetic cipher Decryption

□ Given C= VJJXWPWD

1) Divide Plaintext to three words as your rules number

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

2) C= VJJ XWP WD

3) C= SEC URI TY

Polyalphabetic Ciphers

Vigenère Cipher

Autokey Cipher

Vernam Cipher

Transposition Techniques

Rail Fence Cipher

Row Transposition Cipher

Vigenère cipher

- ❑ The Vigenère cipher, was invented by a Frenchman, Blaise de Vigenère in the 16th century.
- ❑ Vigenère cipher is a simple polyalphabetic cipher

$$\boxed{\quad} \quad C_i = P_i + K \quad \text{mod } 26$$

$$\boxed{\quad} \quad P_i = C_i - K \quad \text{mod } 26$$

- ❑ Repeating key

Vigenère cipher

$$\square \quad C_i = (P_i + K) \bmod 26$$

$$\square \quad P_i = (C_i - K) \bmod 26$$

☐ Repeating key

Vigenère cipher Encryption

❑ K =deceptive

❑ P =we are discovered save yourself

key: *deceptivedeceptivedeceptive*
plaintext: *wearediscoveredsaveyourself*

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

Vigenère cipher Encryption

key: *deceptivedeceptivedeceptive*
plaintext: *wearediscoveredsaveyourself*

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

Vigenère cipher Encryption

❑ Result

key:	<i>deceptivedeceptivedeceptive</i>
plaintext:	wearediscoveredsaveyourself
ciphertext:	ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Vigenère cipher Encryption

- ❑ The strength of Vigenère Cipher is that there are multiple ciphertext letters for each plaintext letter

Vigenère cipher Decryption

❑ decryption simply works in reverse

❑ $P_i = (C_i - K) \bmod 26$

ciphertext:	ZIC <u>VTW</u> QNGRZG <u>VTW</u> AVZHCQYGLMGJ
key:	<i>deceptivedeceptivedeceptive</i>
plaintext:	wearediscoveredsaveyourself

Polyalphabetic Ciphers

Vigenère Cipher

Autokey Cipher

Vernam Cipher

Transposition Techniques

Rail Fence Cipher

Row Transposition Cipher

- ❑ An autokey cipher (also known as the autoclave cipher) is a cipher which incorporates the message (the plaintext) into the key.

- ❑ $P = \{p_1, p_2, p_3, \dots, p_n\}$

- ❑ $K = \{k_1, p_1, p_2, p_3, \dots, p_{n-1}\}$

- ❑ $C = \{c_1, c_2, c_3, \dots, c_n\}$

autokey cipher

$$\square C_i = (P_i + K_i) \bmod 26$$

$$\square P_i = (C_i - K_i) \bmod 26$$

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

autokey cipher Encryption

❑ $K=m$

❑ $P=a$ ttack is today

Plaintext	a	t	t	a	c	k	i	s	t	o	d	a	y
P Value	0	19	19	0	2	10	8	18	19	14	3	0	24
Key	12	0	19	19	0	2	10	8	18	19	14	3	0
C Value	12	19	12	19	2	12	18	0	11	7	17	3	24
Ciphertext	m	t	m	t	c	m	s	a	l	h	r	d	y

autokey cipher Decryption

□ $K=m$

□ $C=mtmtcmsalhrdy$

Ciphertext	m	t	m	t	c	m	s	a	l	h	r	d	y
C Value	12	19	12	19	2	12	18	0	11	7	17	3	24
Key	12	0	19	19	0	2	10	8	18	19	14	3	0
P Value	0	19	19	0	2	10	8	18	19	14	3	0	24
Plaintext	a	t	t	a	c	k	i	s	t	o	d	a	y

Polyalphabetic Ciphers

Vigenère Cipher

Autokey Cipher

Vernam Cipher

Transposition Techniques

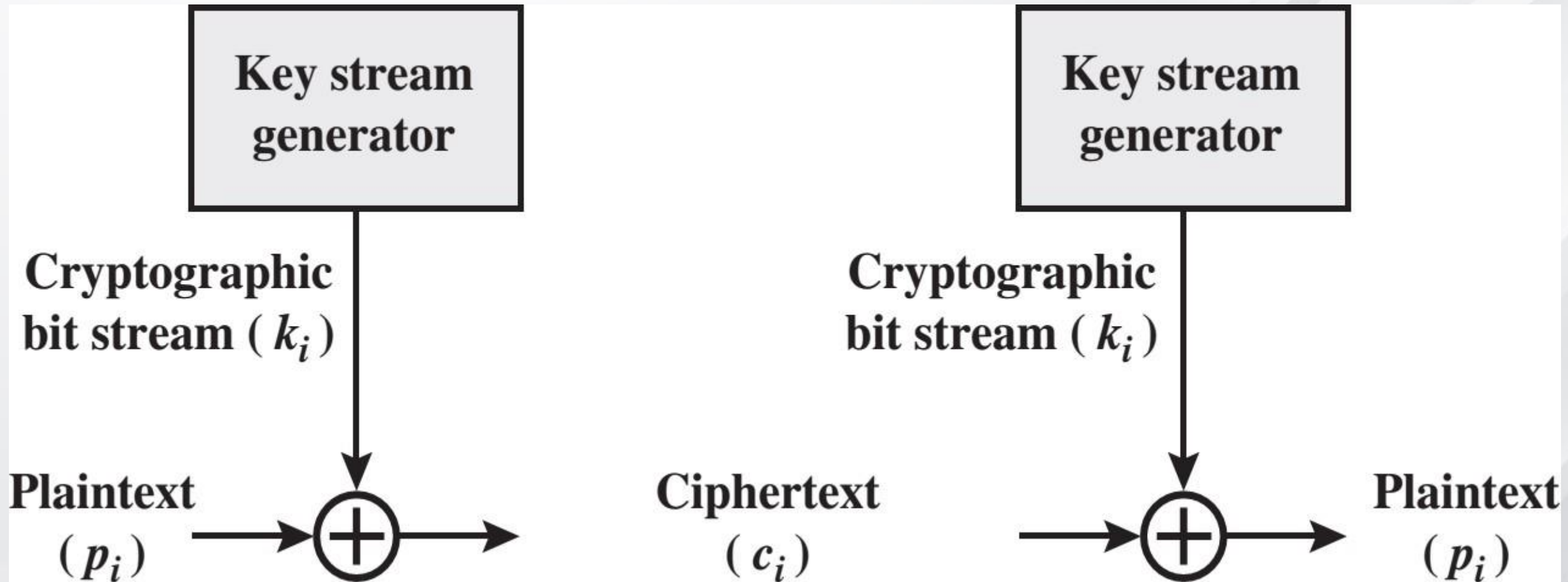
Rail Fence Cipher

Row Transposition Cipher

Vernam cipher

- ❑ Vernam Cipher was introduced by an AT&T engineer named Gilbert Vernam in 1918.
- ❑ The ultimate defense against such a cryptanalysis is to choose a keyword that is as long as the plaintext and has no statistical relationship to it.

Vernam cipher



□ Encryption

➤ $C = P \text{ XOR } K$

□ Decryption

➤ $P = C \text{ XOR } K$

Vernam cipher Encryption

❑ P=11100011101010101101

❑ K=1001010101

❑ P=11100011101010101101

❑ K=10010101011001010101

❑ C=0111011011001111000

Vernam cipher Decryption

- ❑ C=01110110110011111000
- ❑ K=10010101011001010101
- ❑ P=11100011101010101101

Polyalphabetic Ciphers

Vigenère Cipher

Autokey Cipher

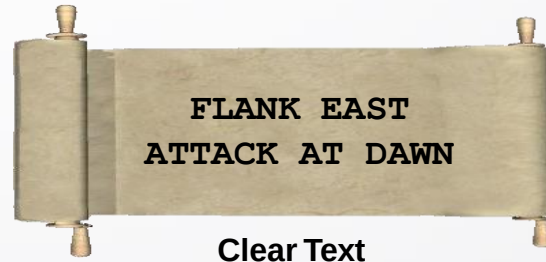
Vernam Cipher

Transposition Techniques

Rail Fence Cipher

Row Transposition Cipher

1



Clear Text

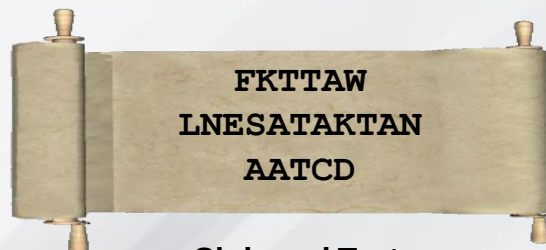
The clear text message would be encoded using a key of 3.

2

F...K...T...T...A...W.
.L.N.E.S.A.T.A.K.T.A.N
..A...A...T...C...D...

Use a rail fence cipher and a key of 3.

3



Ciphered Text

The clear text message would appear as follows.

- ❑ Transposition Techniques performing some sort of permutation on the plaintext letters (reorder the position of letters in plaintext).
- ❑ Types:
 - Rail Fence Cipher
 - Row Transposition Cipher

Polyalphabetic Ciphers

Vigenère Cipher

Autokey Cipher

Vernam Cipher

Transposition Techniques

Rail Fence Cipher

Row Transposition Cipher

Rail Fence Cipher Encryption

- ❑ P= meet me after the toga party
- ❑ K=2

$$1) p = \begin{bmatrix} m & e & m & a & t & r & h & t & g & p & r & y \\ e & t & e & f & e & t & e & o & a & a & t & \end{bmatrix}$$

2) C=mematrhtgpryetefeteoaat

Rail Fence Cipher Decryption

❑ C=mematrhtgpryetefeteoaat

❑ K=2

$$1) C = \begin{bmatrix} m & e & m & a & t & r & h & t & g & p & r & y \\ e & t & e & f & e & t & e & o & a & a & t & \end{bmatrix} \downarrow$$

2) P= meetmeafterthetogaparty

Polyalphabetic Ciphers

Vigenère Cipher

Autokey Cipher

Vernam Cipher

Transposition Techniques

Rail Fence Cipher

Row Transposition Cipher

Row Transposition Cipher Encryption

- ❑ P= attack postponed until two am
- ❑ K= 4312567

$$\square C = \begin{pmatrix} 4 & 3 & 1 & 2 & 5 & 6 & 7 \\ a & t & t & a & c & k & p \\ o & s & t & p & o & n & e \\ d & u & n & t & i & l & t \\ w & o & a & m & x & x & x \end{pmatrix} = ttnaaptmtsuoao dwcoix knl xpetx$$

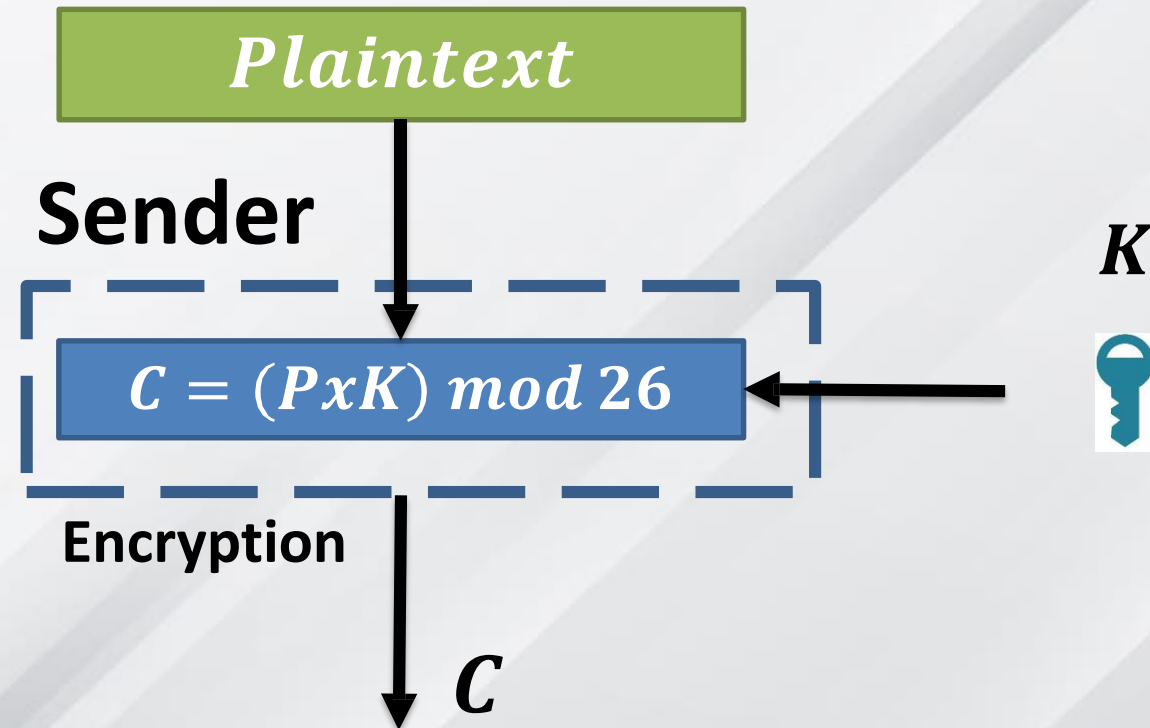
Row Transposition Cipher Decryption

- ❑ $C = \text{ttnaaptmtsuoao dwcoix knl xpetx} = \text{Len}(C) = 28$
- ❑ $K = 4312567$
- ❑ Each Column have $28/7 = 4$ letter

$$\text{❑ } P = \begin{pmatrix} 4 & 3 & 1 & 2 & 5 & 6 & 7 \\ a & t & t & a & c & k & p \\ o & s & t & p & o & n & e \\ d & u & n & t & i & l & t \\ w & o & a & m & x & x & x \end{pmatrix} = \text{attackpostponeduntiltwoamxxx}$$

Task

- As shown in Figure below, use Multiplicative Cipher to encrypt “enemy attack tonight” with key = 4.





مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

