

CYB650

Introduction to Cryptography

Cryptography Techniques



Prepared by Dr. Esraa Saleh Alomari
Lecture #3



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

The Part 1 of the module 2 covers the Cryptography Techniques (Classical Encryption Techniques) are as follows:

- *Conventional Cryptography*
- *Substitution Techniques*
- *Transposition Techniques*
- *Rotor Machines*
- *Steganography*

- ❑ In conventional cryptography, also called *secret-key* or *symmetric-key* encryption, one key is used both for encryption and decryption. The Data Encryption Standard (DES) is an example of a conventional cryptosystem that is widely employed by the U.S. government.

A conventional Cryptography

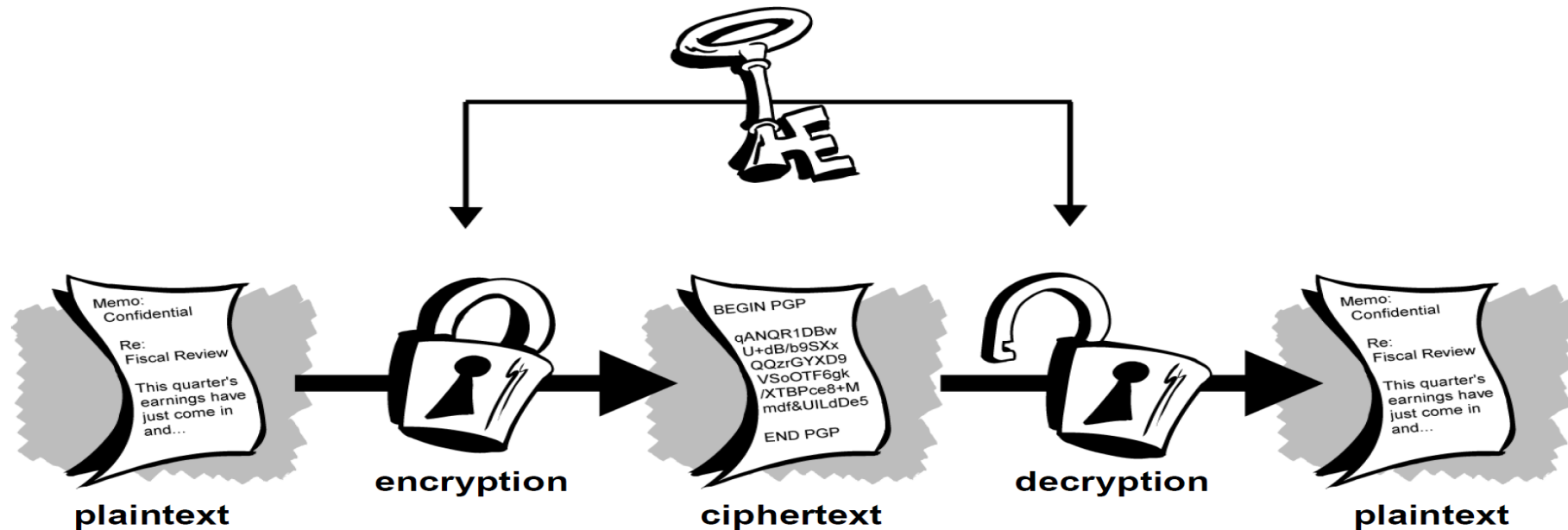


Figure 1: Conventional Cryptography

- ❑ A 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

Substitution Cipher (Caesar's Cipher)

The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

For example,

plain: meet me after the toga party

cipher: PHHW PH DIWHU WKH WRJD SDUWB

Substitution Cipher (Caesar's Cipher)

Note that the alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities, as follows:

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

Substitution Cipher (Caesar's Cipher)

Let us assign a numerical equivalent to each letter:

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 the algorithm can be expressed as follows. For each plaintext letter p substitute the ciphertext letter C



Substitution Cipher (Caesar's Cipher)

$$C = E(3, p) = (p + 3) \bmod 26$$

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

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

If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys. Figure 2 shows the results of applying this strategy to the example ciphertext. In this case, the plaintext leaps out as occupying the third line.

Figure 2: Brute-Force
Cryptanalysis of Caesar
Cipher

KEY	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1	oggv	og	chvgt	vjg	vqic	rectva
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	objv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjllq
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	glzcx	znk	zumg	vgxze
24	rjyy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc



Three important characteristics of this problem enabled us to use a brute-force cryptanalysis:

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily recognizable.

With only **25** possible keys, the Caesar cipher is far from secure. A dramatic increase in the key space can be achieved by allowing an arbitrary substitution. Before proceeding, we define the term ***permutation***. A **permutation** of a finite set of elements S is an ordered sequence of all the elements of S 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

Caesar's Cipher – Monoalphabetic Cipher

In general, there are $n!$ permutations of a set of n elements, because the first element can be chosen in one of n ways, the second in $n-1$ ways, the third in $n-2$ ways, and so on.

Recall the assignment for the Caesar 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:	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

If, instead, the “cipher” line can be any permutation of the 26 alphabetic characters, then there are $26!$ or greater than $4 * 10^{26}$ possible keys. This is 10 orders of magnitude greater than the key space for DES and would seem to eliminate brute-force techniques for cryptanalysis. Such an approach is referred to as a **monoalphabetic substitution cipher**, because a single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.



There is, however, another line of attack. If the cryptanalyst knows the nature of the plaintext (e.g., non-compressed English text), then the analyst can exploit the regularities of the language. The ciphertext to be solved is

**UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAI Z
VUEPHZHMDZSHZOWSFPAPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ**

Two principal methods are used in substitution ciphers to lessen the extent to which the structure of the plaintext survives in the ciphertext:

- One approach is to encrypt multiple letters of plaintext
- Use multiple cipher alphabets

The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.

The Playfair algorithm is based on the use of a 5 * 5 matrix of letters constructed using a keyword. Here is an example, solved by Lord Peter Wimsey in Dorothy Sayers's *Have His Carcase*:

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

In this case, the keyword is ***monarchy***. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters ***I*** and ***J*** count as one letter.



Plaintext is encrypted two letters at a time, according to the following rules:

1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.

2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.
3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.

4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

- The Playfair cipher is a great advance over simple monoalphabetic ciphers. For one thing, whereas there are only 26 letters, there are $26 * 26 = 676$ diagrams, so that identification of individual diagrams is more difficult
- Furthermore, the relative frequencies of individual letters exhibit a much greater range than that of diagrams, making frequency analysis much more difficult

- For these reasons, the Playfair cipher was for a long time considered unbreakable. It was used as the standard field system by the British Army in World War I and still enjoyed considerable use by the U.S. Army and other Allied forces during World War II.

- Despite this level of confidence in its security, the Playfair cipher is relatively easy to break, because it still leaves much of the structure of the plaintext language intact. A few hundred letters of ciphertext are generally sufficient.

- ✓ Multi- Layer Cipher
- ✓ Developed by the mathematician Lester Hill in 1929
- ✓ Encrypts a group of letters : digraph , trigraph or polygraph

- ❑ Review few terminologies from linear algebra
- ❑ Concepts to be known
 - Matrix arithmetic modulo 26
 - Square Matrix
 - Determinant
 - Multiplicative inverse

- This can be expressed as :

$$C=E(K,P) = P*K \bmod 26$$

$$P=D(K,C) = C K^{-1} \bmod 26 = P * K * K^{-1} \bmod 26$$

$$(C_1, C_2, C_3) = (P_1, P_2, P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

Encryption

$$C_1 = (P_1 K_{11} + P_2 K_{21} + P_3 K_{31}) \bmod 26$$

$$C_2 = (P_1 K_{12} + P_2 K_{22} + P_3 K_{32}) \bmod 26$$

$$C_3 = (P_1 K_{13} + P_2 K_{23} + P_3 K_{33}) \bmod 26$$



Hill Cipher Example

Question: Encrypt "pay more money" using hill cipher with key

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Solution:

p	a	y	m	o	r	e	m	o	n	e	y
15	0	24	12	14	17	4	12	14	13	4	24

*Key= 3*3 Matrix*

PT= pay mor emo ney



Hill Cipher Example

Encryption :pay

$$(C_1, C_2, C_3) = (P_1, P_2, P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \text{mod } 26$$

$$(C_1, C_2, C_3) = (15 \ 0 \ 24) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \text{mod } 26$$

$$= (15*17+0*21+24*2 \quad 15*17+15*18+15*2 \quad 15*5+15*21+15*19) \text{ mod } 26$$

$$= (303 \ 303 \ 531) \text{ mod } 26$$

$$= (17 \ 17 \ 11)$$

$$= (R \ R \ L)$$



Encryption :mor

$$(C_1, C_2, C_3) = (P_1, P_2, P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \text{mod } 26$$

$$(C_1, C_2, C_3) = (12 \ 14 \ 17) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \text{mod } 26$$

$$= (12*17+14*21+17*2 \quad 12*17+14*18+17*2 \quad 12*5+14*21+17*19) \text{ mod } 26$$

$$= (532 \ 490 \ 677) \text{ mod } 26$$

$$= (12 \ 22 \ 1)$$

$$= (M \ W \ B)$$



Hill Cipher Example

Encryption :emo

$$(C_1, C_2, C_3) = (P_1, P_2, P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \text{mod } 26$$

$$(C_1, C_2, C_3) = (4 \ 12 \ 14) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \text{mod } 26$$

$$= (4*17+12*21+14*2 \quad 4*17+12*18+14*2 \quad 4*5+12*21+14*19) \text{ mod } 26$$

$$= (348 \ 312 \ 538) \text{ mod } 26$$

$$= (10 \ 0 \ 18)$$

$$= (K \ A \ S)$$



Encryption :ney

$$(C_1, C_2, C_3) = (P_1, P_2, P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \text{mod } 26$$

$$(C_1, C_2, C_3) = (13 \ 4 \ 24) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \text{mod } 26$$

$$= (13*17+4*21+24*2 \quad 13*17+4*18+24*2 \quad 13*5+4*21+24*19) \text{ mod } 26$$

$$= (348 \ 312 \ 538) \text{ mod } 26$$

$$= (15 \ 3 \ 7)$$

$$= (P \ D \ H)$$



Hill Cipher Example

p	a	y	m	o	r	e	m	o	n	e	y
R	R	L	M	W	B	K	A	S	P	D	H

An Army Signal Corp officer, Joseph Mauborgne, proposed an improvement to the Vernam cipher that yields the ultimate in security. Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated. In addition, the key is to be 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. Such a scheme, known as a one-time pad, is unbreakable. It 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.



All the techniques examined so far involve the substitution of a ciphertext symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. For example, to encipher the message “meet me after the toga party” with a rail fence of depth 2, we write the following:

Transposition Techniques

m e m a t r h t g p r y
e t e f e t e o a a t

The encrypted message is

MEMATRHTGPRYETEFETEOAAT



Transposition Techniques

This sort of thing would be trivial to cryptanalyze. 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. For example,

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



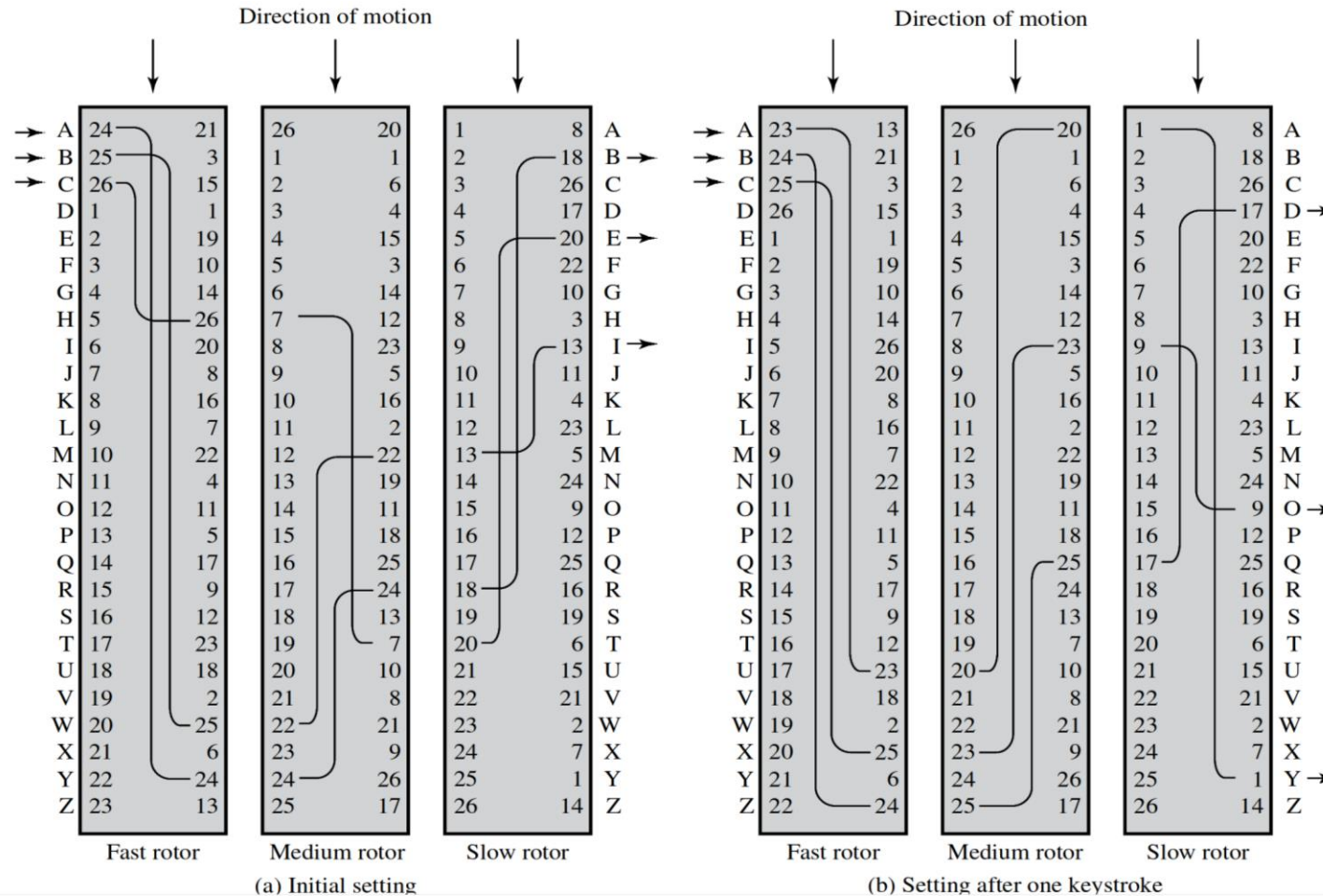
The basic principle of the rotor machine is illustrated in Figure 2.8.

The machine consists of a set of independently rotating cylinders through which electrical pulses can flow. Each cylinder has 26 input pins and 26 output pins, with internal wiring that connects each input pin to a unique output pin.



For simplicity, only three of the internal connections in each cylinder are shown. If we associate each input and output pin with a letter of the alphabet, then a single cylinder defines a monoalphabetic substitution. For example, in Figure 2.8, if an operator depresses the key for the letter A, an electric signal is applied to

ROTOR Machines



A plaintext message may be hidden in one of two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.

Thank You

ANY
QUESTIONS?

