الجامعة المستنصرية /كلية التربية / قسم علوم الحاسبات

4th Class
Computers & Data Security
أمنية الحاسوب والبيانات

أستاذ المادة

أ.م . د . اخلاص عباس البحراني

Chapter Three
Classical Symmetric Cipher

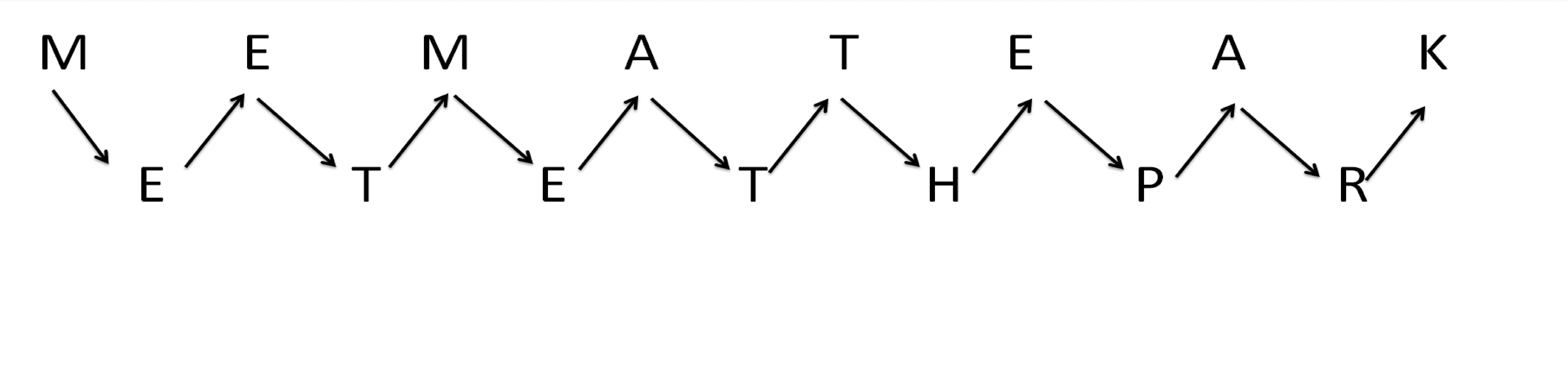
اعداد: أ.م.د. اخلاص البحراني

The forms of Encryption

- **Transposition (or permutation) cipher:** Transposition cipher keeps the letters the same, but rearranges their order according to a specific algorithm.
- **Substitution cipher:** replacing each element of the plaintext with another element.
- **Product cipher:** using multiple stages of substitutions and transpositions

Transposition cipher

1. **Keyless Transposition Ciphers:** - Simple transposition ciphers, which were used in the past, are keyless. A good example of a keyless cipher using the first method is the **rail fence cipher.** The ciphertext is created reading the pattern row by row. For example, to send the message (**Meet me at the park**) to Bob, Alice writes



- She then creates the ciphertext (**MEMATEAKETETHPR**).

2. Columnar Transposition Ciphers.

- Write the message in rows of a fixed length, and then read out again column by column.
- The columns are chosen in some scrambled order.
- Both the length of the rows and the permutation of the columns are usually defined by a key.

<u>Example:</u> Let the plaintext is (WE ARE DISCOVERED FLEE AT ONCE) the key word be: ZEBRA.

Z	E	B	R	A
W	E	A	R	E
D	I	S	C	O
V	E	R	E	D
F	L	E	E	A
T	O	N	C	E

- The ciphertext:

EODAEASRENEIELORCEECWDVFT

Double Columnar Transposition.

اعداد: أ.م.د. اخلاص البحراني

Substitution cipher

1. **Monoalphabetic Ciphers.**
   - It is simple substitution
   - involves replacing each letter in the message with another letter of the alphabet.
   - In monoalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.

- **Additive Cipher:-** is the simplest monoalphabetic cipher. It is sometimes called a shift cipher and sometimes **a Caesar cipher**, but the term additive cipher better reveals its mathematical nature. When the cipher is additive, the plaintext, ciphertext, and key are integers in Z26.

Plaintext and ciphertext in Z26

Plaintext →	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 →	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
Value →	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

Additive Cipher

- ***Example***
- Use the additive cipher with key = 15 to encrypt the plain text (hello).
- We apply the encryption algorithm to the plaintext, character by character:

Plaintext h e l l o

7 4 11 11 14

Encryption

(7+15) mod 26=22→ W, (4+15) mod 26=19 →T, (11 +15) mod 26=0 →A, (11+15) mod 26=0 →A,(14+15) mod 26=3 →D

Ciphertext WTAAD

- We apply the decryption algorithm to the plaintext character by character:

Ciphertext

W T A A D

22 19 0 0 3

Decryption

(22-15) mod 26=7→ h, (19-15) mod 26=4 →e, (0-15) mod 26=11 →l, (0-15) mod 26=11 →l,(3-15) mod 26=14 →o

Ciphertext h e l l o

اعداد: أ.م.د. اخلاص البحراني

- **Caesar Cipher: -** Named for Julious Caesar. Caesar used a key of 3 for his communications.

Plaintext 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 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

- **Cryptanalysis of the Caesar cipher: -**

- Example : - decrypt the following ciphertext:-
  wklv phvvdjh lv qrw wrr kdug wr euhdn
- By using the above table, replace the characters as show
  ciphertext = wklv phvvdjh lv qrw wrr kdug wr euhdn
  plaintext = THIS MESSAGE IS NOT TOO HARD TO BREAK

- \`

- ***Example:*** Eve has intercepted the ciphertext (UVACLYFZLJBYL). Show how she can use a brute-force attack to break the cipher.
- Eve tries keys from 1 to 7. With a key of 7, the plaintext is (not very

Ciphertext: UVACLYFZLJBYL

K = 1	$\longrightarrow$	**Plaintext:** tuzbkxeykiaxk
K = 2	$\longrightarrow$	**Plaintext:** styajwdxjhzwj
K = 3	$\longrightarrow$	**Plaintext:** rsxzivcwigyvi
K = 4	$\longrightarrow$	**Plaintext:** qrwyhubvhfxuh
K = 5	$\longrightarrow$	**Plaintext:** pqvxgtaugewtg
K = 6	$\longrightarrow$	**Plaintext:** opuwfsztfdvsf
K = 7	$\longrightarrow$	**Plaintext:** notverysecure

Table of Frequency of characters in English

Letter	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Frequency distributions of Plaintext :-

- E
- T
- A, O, R, N , I
- H , C , D , L, M
- .
- .
- X , J ,Z , Q

- Example : - Eve has intercepted the following ciphertext. Using a statistical attack, find the plaintext.

Ciphertext= hqfubswlrq lv d phdqv ri dwwdlqlqj vhfxuh frppxulfdwlrq

- When Eve tabulates the frequency of letters in this ciphertext, she gets:

h=26, v=17 and so on.

Frequencies of characters

Letter	Count	Percent	Letter	Count	Percent
a	0	0.00	n	0	0.00
b	3	1.80	o	4	2.41
c	0	0.00	p	5	2.99
d	11	6.59	q	16	9.58
e	2	1.20	r	9	5.39
f	6	3.61	s	3	1.80
g	4	2.40	t	0	0.00
h	26	15.56	u	8	4.79
i	2	1.20	v	17	10.18
j	5	2.99	w	14	8.38
k	5	2.99	x	5	2.99
l	16	9.58	y	4	2.40
m	0	0.00	z	2	1.20

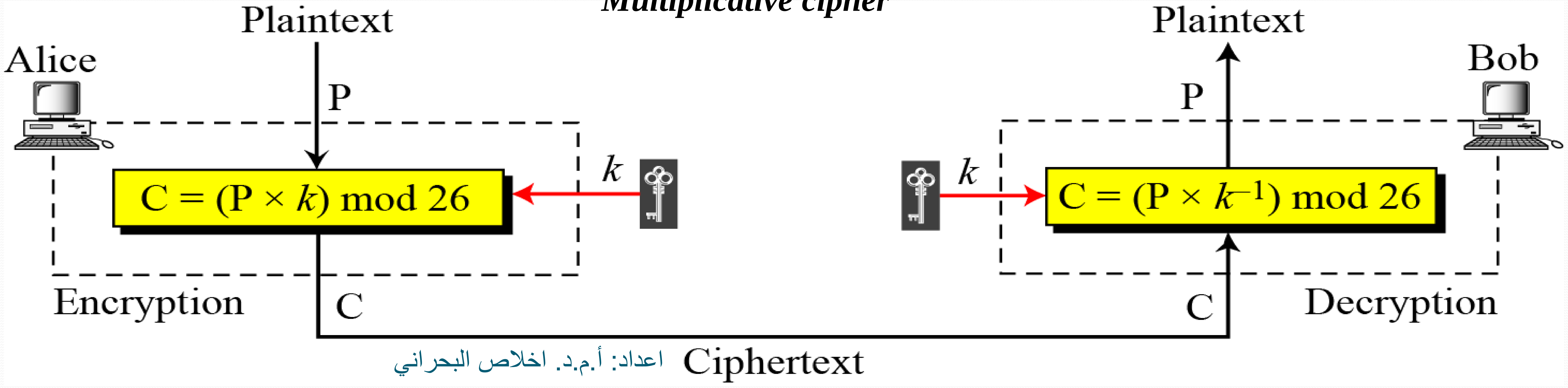
- So we will replace each character with the corresponding high frequency in plaintext as shown: -

Plaintext = ENCRYPTION IS A MEANS OF ATTAINING SECURE COMMUNICATION

Which means that the key is =3 ? How?

- **Multiplicative Ciphers:** - In a multiplicative cipher, the plaintext and ciphertext are integers in Z_{26}; the key is an integer in Z_{26}^*.

Multiplicative cipher



- The key domain for any multiplicative cipher which must be in Z_{26}^*, is the set that has only 12 members: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.(**why**)
- Example: - We use a multiplicative cipher to encrypt the message "hello" with a key of 7. The ciphertext is "XCZZU".

Plaintext: h $\rightarrow$ 07	Encryption: (07×07) mod 26	ciphertext: 23 $\rightarrow$ X
Plaintext: e $\rightarrow$ 04	Encryption: (04×07) mod 26	ciphertext: 02 $\rightarrow$ C
Plaintext: l $\rightarrow$ 11	Encryption: (11×07) mod 26	ciphertext: 25 $\rightarrow$ Z
Plaintext: l $\rightarrow$ 11	Encryption: (11×07) mod 26	ciphertext: 25 $\rightarrow$ Z
Plaintext: o $\rightarrow$ 14	Encryption: (14×07) mod 26	ciphertext: 20 $\rightarrow$ U

- Cryptanalyses of the multiplicative cipher based on finding the multiplication inverse of the key (where the multiplication inverse of **7 is 15**) as shown

Ciphertext X $\rightarrow$ 23	Decryption: (23 * 15) mod 26	plaintext= 7$\rightarrow$h
Ciphertext C $\rightarrow$ 2	Decryption: (2 * 15) mod 26	plaintext= 4$\rightarrow$e
Ciphertext Z $\rightarrow$ 25	Decryption: (25 * 15) mod 26	plaintext=11$\rightarrow$l
Ciphertext Z $\rightarrow$ 25	Decryption: (25 * 15) mod 26	plaintext=11$\rightarrow$l
Ciphertext U $\rightarrow$ 20	Decryption: (20 * 15) mod 26	plaintext=14$\rightarrow$o

- Affine Ciphers

$$C = (P \times k_1 + k_2) \bmod 26 \qquad P = ((C - k_2) \times k_1^{-1}) \bmod 26$$

where k_1^{-1} is the multiplicative inverse of k_1 and $-k_2$ is the additive inverse of k_2

- The affine cipher uses a pair of keys in which the first key is from Z_{26}^* and the second is from Z_{26}. The size of the key domain is $26 \times 12 = 312$.
- The additive cipher is a special case of an affine cipher in which $k_1 = 1$. The multiplicative cipher is a special case of affine cipher in which $k_2 = 0$.

- Example: - Use an affine cipher to encrypt the message “hello” with the key pair (7, 2).

P: h $\rightarrow$ 07	Encryption: $(07 \times 7 + 2) \bmod 26$	C: 25 $\rightarrow$ Z
P: e $\rightarrow$ 04	Encryption: $(04 \times 7 + 2) \bmod 26$	C: 04 $\rightarrow$ E
P: l $\rightarrow$ 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 $\rightarrow$ B
P: l $\rightarrow$ 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 $\rightarrow$ B
P: o $\rightarrow$ 14	Encryption: $(14 \times 7 + 2) \bmod 26$	C: 22 $\rightarrow$ W

- To decrypt the message “ZEBBW” with the key pair (7, 2) in modulus 26. where where the multiplication inverse of **7 is 15**

C: Z $\rightarrow$ 25	Decryption: $((25 - 2) \times 7^{-1}) \bmod 26$	P:07 $\rightarrow$ h
C: E $\rightarrow$ 04	Decryption: $((04 - 2) \times 7^{-1}) \bmod 26$	P:04 $\rightarrow$ e
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 $\rightarrow$ l
C: B $\rightarrow$ 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 $\rightarrow$ l
C: W $\rightarrow$ 22	Decryption: $((22 - 2) \times 7^{-1}) \bmod 26$	P:14 $\rightarrow$ o

2. Polyalphabetic Ciphers

- In polyalphabetic substitution, each occurrence of a character may have a different substitute.
- The relationship between a character in the plaintext to a character in the ciphertext is one-to-many.
- **Autokey Cipher: -**

$$P = P_1P_2P_3 \ldots \qquad C = C_1C_2C_3 \ldots \qquad k = (k_1, P_1, P_2, \ldots)$$

$$\text{Encryption: } C_i = (P_i + k_i) \bmod 26 \qquad \text{Decryption: } P_i = (C_i - k_i) \bmod 26$$

- Assume that Alice and Bob agreed to use an autokey cipher with initial key value $k_1 = 12$. Now Alice wants to send Bob the message "Attack is today". Enciphering is done character by character as shown :-

Plaintext:	a	t	t	a	c	k	i	s	t	o	d	a	y
P's Values:	00	19	19	00	02	10	08	18	19	14	03	00	24
Key stream:	*12*	*00*	*19*	*19*	*00*	*02*	*10*	*08*	*18*	*19*	*14*	*03*	*00*
C's Values:	12	19	12	19	02	12	18	00	11	7	17	03	24
Ciphertext:	**M**	**T**	**M**	**T**	**C**	**M**	**S**	**A**	**L**	**H**	**R**	**D**	**Y**

- **Vigenere Cipher: -**

$P = P_1P_2P_3 \ldots \qquad C = C_1C_2C_3 \ldots \qquad K = [(k_1, k_2, \ldots, k_m), (k_1, k_2, \ldots, k_m), \ldots]$

Encryption: $C_i = P_i + k_i$ Decryption: $P_i = C_i - k_i$

- **Example: -** We can encrypt the message "She is listening" using the 6-character keyword "PASCAL".

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***
C's values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**

- Vigenere cipher can be seen as combinations of m additive ciphers. As shown in a Vigenere Tableau which can be used to find ciphertext which the intersection of a row and column.

	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	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

- **Running Key:** -Exactly Vigenere Cipher but the key length is exactly same length of the plaintext, usually keys are determined from books known from both sender and receiver.

3. Polygraphic Ciphers

- Instead of substituting one letter for another letter, a polygraphic cipher performs substitutions with two or more groups of letters.
- This has the advantage of masking the frequency distribution of letters, which makes frequency analysis attackes much more difficult.
- **Playfair Cipher:-** You create 5x5 matrix based on a keyword with the reset of the alphabets characters. For example a keyword (without repetition) such as "PROBLEMS":

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

- In this cipher, we will encipher letters pairs at a time. Consider the following plaintext:

  SHE WENT TO THE STORE

- When we pair up the letters they get grouped as follows:

  SH EW EN TT OT HE ST OR E

- But, we are not allowed to encipher any double letters. So, in this case, we will insert an Q into the plaintext. (If Q is a double letter, then insert another infrequent letter, say X.)

  SH EW EN TQ TO TH ES TO RE

- To encipher pairs of letters, adhere to the following rules:

1. If the two letters are on the same row of the chart, like "ES", then replace each letter by the letter to the right. (If necessary, wrap around to the left end of the row. So "ES" encrypts to "MA".

2. If the two letters are on the same column of the chart, like, "TH", then replace each letter by the letter below it. (If necessary, wrap around to the top end of the column.) So "TH" encrypts to "YT".

3. If two letters are on a different row and column, like, "SH", then replace each letter by another letter on its same row, but in the column of the other letter. So "SH" encrypts to "AG".

- Using these rules, here is the encryption of the plaintext above:

Plaintext : SH EW EN TQ TO TH ES TO RE

Ciphertext: AG MV MK UT QB YT MA QB PM

- To decipher, ignore rule 1. In rules 2 and 3 shift up and left instead of down and right. Rule 4 remains the same. Once you are done, drop any extra Xs that don't make sense in the final message and locate any missing Qs or any Is that should be Js.

Hill Cipher

- ***CONCEPTS FROM LINEAR ALGEBRA:*** The Hill Cipher uses matrix multiplication modulo 26 to encrypt a message.
- First, you need to assign two numbers to each letter in the alphabet and also assign numbers to space, . , and ? or !.
- The key space is the set of all invertible matrices over Z_{26}. 26 was chosen because there are 26 characters, which solves some problems later on.

$$K = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix}$$

$$\begin{aligned} C_1 &= P_1 k_{11} + P_2 k_{21} + \cdots + P_m k_{m1} \\ C_2 &= P_1 k_{12} + P_2 k_{22} + \cdots + P_m k_{m2} \\ &\cdots \\ C_m &= P_1 k_{1m} + P_2 k_{2m} + \cdots + P_m k_{mm} \end{aligned}$$

- the Hill system can be expressed as $\mathbf{C} = E(\mathbf{K}, \mathbf{P}) = \mathbf{PK} \bmod 26$

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

- The key matrix in the Hill cipher needs to have a multiplicative inverse.

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

$$\mathbf{AA}^{-1} = \begin{pmatrix} (5 \times 9) + (8 \times 1) & (5 \times 2) + (8 \times 15) \\ (17 \times 9) + (3 \times 1) & (17 \times 2) + (3 \times 15) \end{pmatrix}$$

$$= \begin{pmatrix} 53 & 130 \\ 156 & 79 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Inverse of a matrix

- To explain how the inverse of a matrix is computed, we begin with the concept of determinant.
- For any square matrix ($m * m$), the **determinant** equals the sum of all the products that can be formed by taking exactly one element from each row and exactly one element from each column, with certain of the product terms preceded by a minus sign.
- For a 2 * 2 matrix,

$$\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$$

- The determinant is $k_{11} * k_{22} - k_{12} * k_{21}$.
- For a 3 * 3 matrix, the value of the determinant is $k_{11} * k_{22} * k_{33} + k_{21} * k_{32} * k_{13} + k_{31} * k_{12} * k_{23} - k_{31} * k_{2} * 2k_{13} - k_{21} * k_{12} * k_{33} - k_{11} * k_{32} * k_{23}$.
- If a square matrix **A** has a nonzero determinant, then the inverse of the matrix is computed as

$$[\mathbf{A}^{-1}]_{ij} = (\det \mathbf{A})^{-1}(-1)^{i+j}(\mathbf{D}_{ji}).$$

- where (D_{ji}) is the subdeterminant formed by deleting the jth row and the ith column of **A**, det(**A**) is the determinant of **A**, and (det **A**)$^{-1}$ is the multiplicative inverse of (det **A**) mod 26.

- Continuing our example,

$$\det\begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix} = (5 \times 3) - (8 \times 17) = -121 \bmod 26 = 9$$

- We can show that $9^{-1} \bmod 26 = 3$, because $9 * 3 = 27 \bmod 26 = 1$.
- Therefore, we compute the inverse of **A** as

$$\mathbf{A} = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$$

$$\mathbf{A}^{-1} \bmod 26 = 3\begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix} = 3\begin{pmatrix} 3 & 18 \\ 9 & 5 \end{pmatrix} = \begin{pmatrix} 9 & 54 \\ 27 & 15 \end{pmatrix} = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$$

- For example, consider the plaintext “paymoremoney” and use the encryption key

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

- The encryption process can be expressed as

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

- or

C = **PK** mod 26

- where **C** and **P** are row vectors of length 3 representing the plaintext and ciphertext, and **K** is a 3 * 3 matrix representing the encryption key. Operations are performed mod 26.

- The first three letters of the plaintext are represented by the vector (15 0 24).
- Then (15 0 24)**K** = (303 303 531) mod 26 = (17 17 11) = RRL.
- Continuing in this fashion, the ciphertext for the entire plaintext is RRLMWBKASPDH.
- Decryption requires using the inverse of the matrix **K**. We can compute det **K** = 23, and therefore, $(\det \mathbf{K})^{-1}$ mod 26 = 17. We can then compute the inverse as

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

- This is demonstra

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

- Homework : recover the plaintext.
- Although the Hill cipher is strong against a ciphertext-only attack, it is easily broken with a known plaintext attack.

- For example, the plaintext “code is ready” can make a 3×4 matrix when adding extra bogus character “z” to the last block and removing the spaces.

$$\overset{C}{\begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix}} = \overset{P}{\begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix}} \overset{K}{\begin{bmatrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \\ 03 & 23 & 21 & 08 \end{bmatrix}}$$

a. Encryption

$$\overset{P}{\begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix}} = \overset{C}{\begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix}} \overset{K^{-1}}{\begin{bmatrix} 02 & 15 & 22 & 03 \\ 15 & 00 & 19 & 03 \\ 09 & 09 & 03 & 11 \\ 17 & 00 & 04 & 07 \end{bmatrix}}$$

b. Decryption

- The ciphertext is “OHKNIHGKLISS”.
-

- The first three letters of the plaintext are represented by the vector (15 0 24).
- Then (15 0 24)**K** = (303 303 531) mod 26 = (17 17 11) = RRL.
- Continuing in this fashion, the ciphertext for the entire plaintext is RRLMWBKASPDH.
- Decryption requires using the inverse of the matrix **K**. We can compute det **K** = 23, and therefore, (det **K**)$^{-1}$ mod 26 = 17. We can then compute the inverse as

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

- This is demonstrated as

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

- Homework : recover the plaintext.
- Although the Hill cipher is strong against a ciphertext-only attack, it is easily broken with a known plaintext attack. اعداد: أ.م.د. اخلاص البحراني

- **One-Time Pad**: - One of the goals of cryptography is perfect secrecy. A study by Shannon has shown that perfect secrecy can be achieved if each plaintext symbol is encrypted with a key randomly chosen from a key domain. This idea is used in a cipher called one-time pad, invented by **Vernam.**
- **Example**:- Plaintext VERNAMCIPHER
- **Key** 76 48 16 82 44 3 58 11 60 5 48 88
- **Encryption**

Plaintext 21 4 17 13 0 12 2 8 15 7 4 17

+

Key 76 48 16 82 44 3 58 11 60 5 48 88

Ciphertext 97 52 33 95 44 15 60 19 75 12 52 105 mod 26

19 0 7 17 18 15 8 19 23 12 0 1

t a h r s p i t x m a b

- # Decryption

Ciphertext	t	a	h	r	s	p	i	t	x	m	a	b	
	19	0	7	17	18	15	8	19	23	12	0	1	
												-	
Key	76	48	16	82	44	3	58	11	60	5	48	88	
plaintext	-57	-48	-9	-65	-26	12	-50	8	-37	7	-48	-87	mod 26
	21	4	17	13	0	12	2	8	15	7	4	17	
	V	E	R	N	A	M	C	I	P	H	E	R	