CRYPTOGRAPHY

LECTURE FOUR

Classical (Traditional) Encryption Techniques (cont.)

Substitution cipher

Assis prof. Dr. Saja J. Mohammed

2025-2024

Substitution cipher

In the substitution technique the letters of plaintext are replaced by other (letters or by numbers or symbols).

In general, it can be classified in to two types :

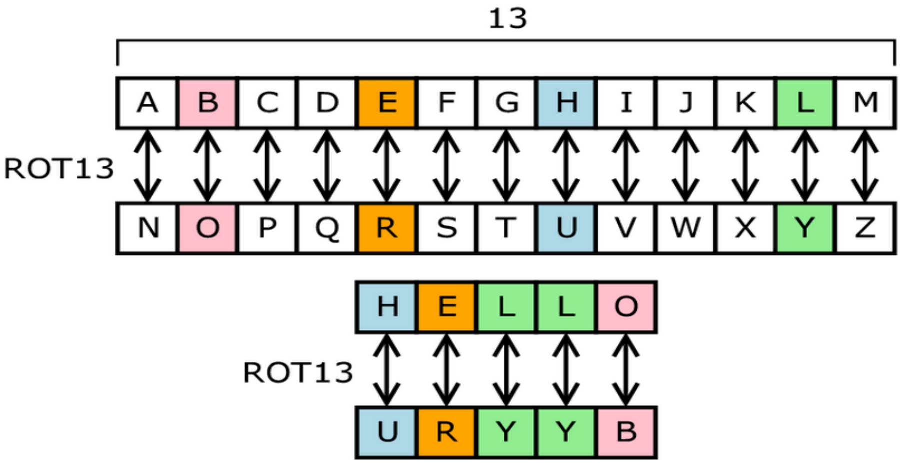
1. Monoalphabetic cipher.
2. Polyalphabetic cipher.

Monoalphabetic cipher

Each character of a plaintext is mapped to a fixed other character of cipher text. The relationship between a character in the plaintext and the characters in the cipher text is one-to-one.

Example :

If a plaintext has a character **‘a’** and any key then if it convert into other character say **‘t’** so wherever there is **‘a’** character in plaintext it will be mapped to character **‘t’**. Therefore it is called as monoalphabetic cipher.



Polyalphabetic cipher:

It is any cipher based on substitution, using several substitution alphabets. In polyalphabetic substitution ciphers, the plaintext letters are enciphered differently based upon their position in the plaintext. Rather than being a one-to-one correspondence, there is a one-to-many relationship between each letter and its substitutes.

For example: **‘a’** can be enciphered as **‘d’** in the starting of the text, but as **‘n’** at the middle.

The polyalphabetic ciphers have the benefit of hiding the letter frequency of the basic language. Therefore attacker cannot use individual letter frequency static to divide the ciphertext.

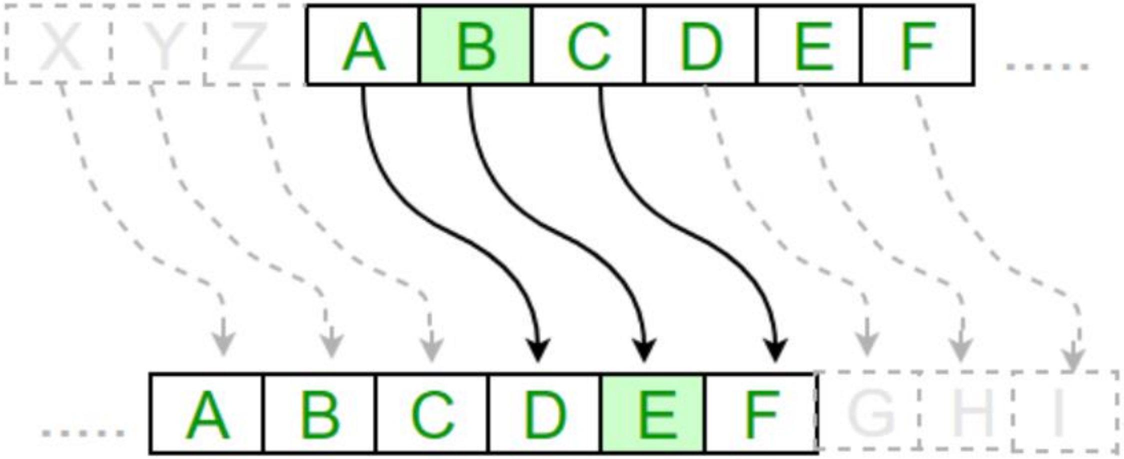
Monoalphabetic vs polyalphabetic

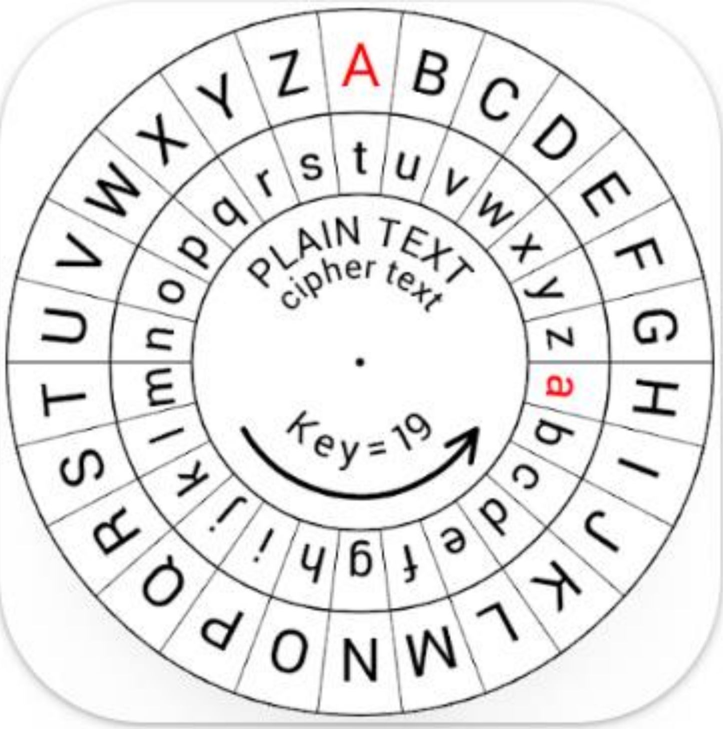
	Monoalphabetic cipher	Polyalphabetic cipher
Basics	Once the key is chosen each alphabetic character of a plaintext is mapped onto a UNIQUE alphabetic character of a cipher text.	Each alphabetic character of a plaintext can be mapped onto 'm' alphabetic characters of a ciphertext.
Relationship between plaintext and cipher text	The relationship between a character in the plaintext and the character in the ciphertext is one to one.	The relationship between a character in the plaintext and the character in the ciphertext is one to many.
Examples	Monoalphabetic cipher includes additive, caesar cipher and affine cipher algorithm.	Polyalphabetic cipher includes playfair, vigenere, Hill and one time pad cipher.
Strength	It has less strength if compare with polyalphabetic cipher	It considers more strong if compare with mono alphabetic cipher

Monoalphabetic cipher algorithms

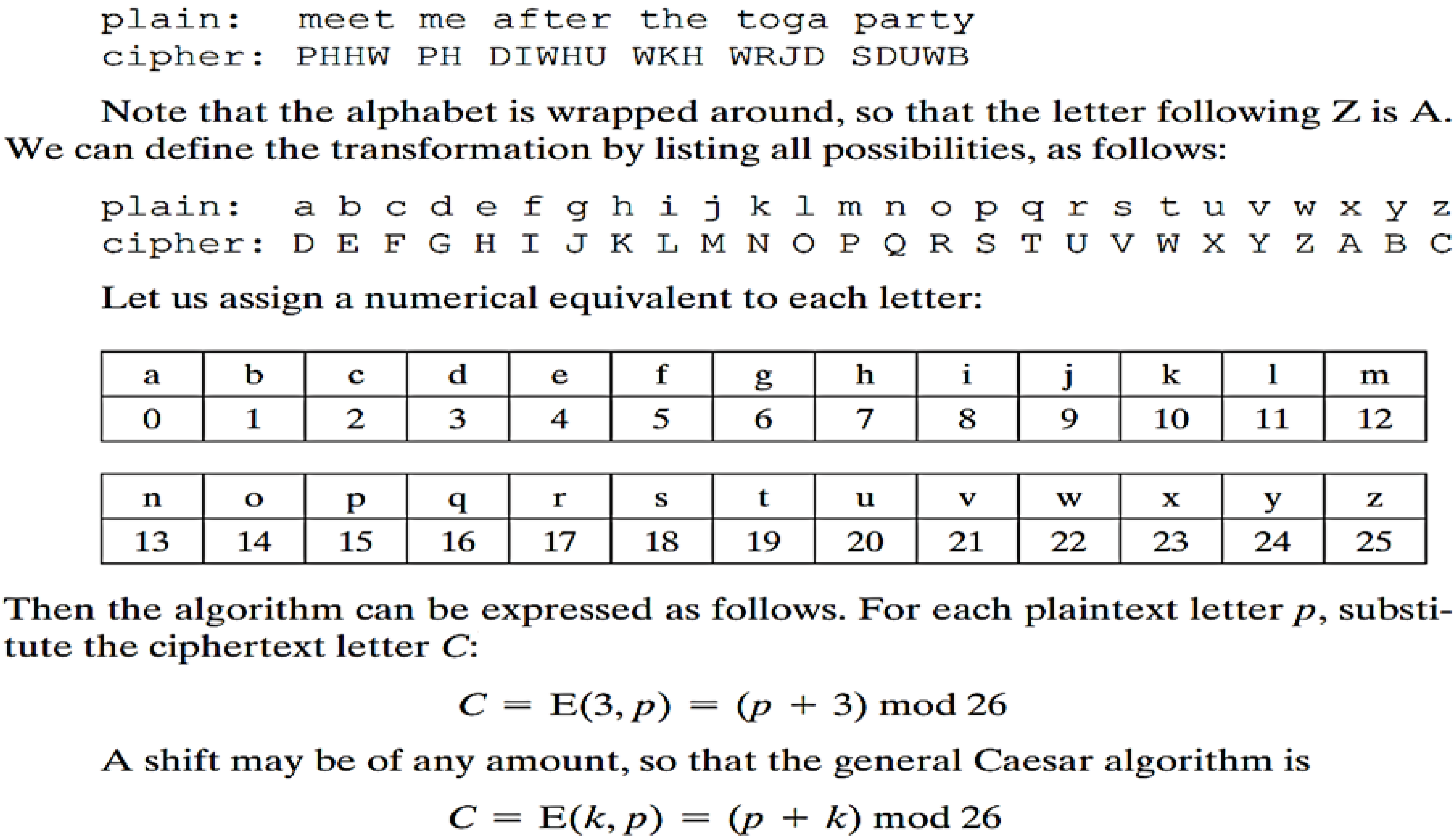
1. *Caesar Cipher*

The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example,





Caesar Cipher



```
plain:   meet me after the toga party
cipher:  PHHW PH DIWHU WKH WRJD SDUWB
```

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
```

Let us assign a numerical equivalent to each letter:

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

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

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

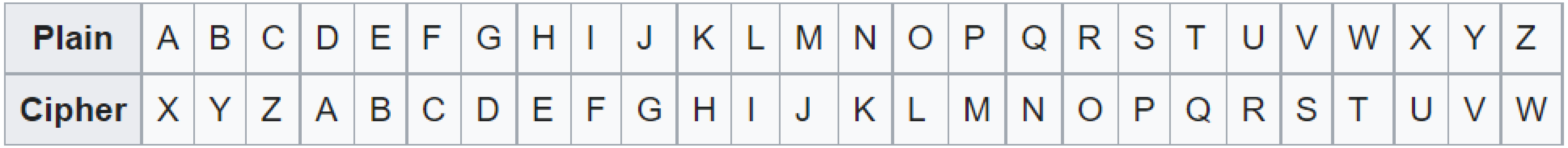
A shift may be of any amount, so that the general Caesar algorithm is

$$C = \mathrm{E}(k, p) = (p + k) \bmod 26$$

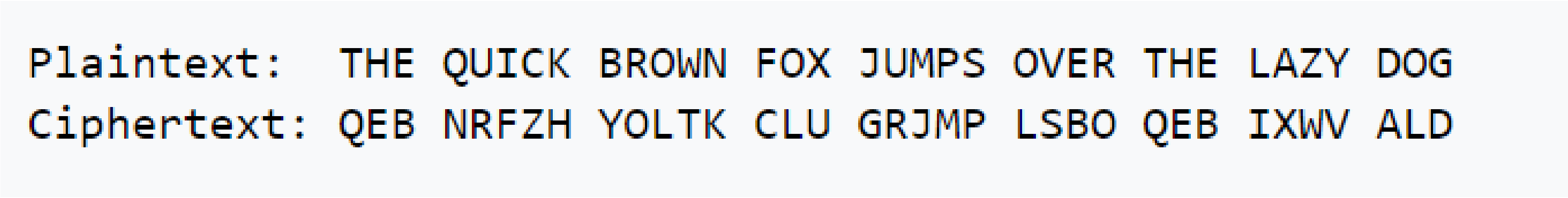
$$P = D(k,c)=(c-k) \bmod 26$$

Caesar Cipher

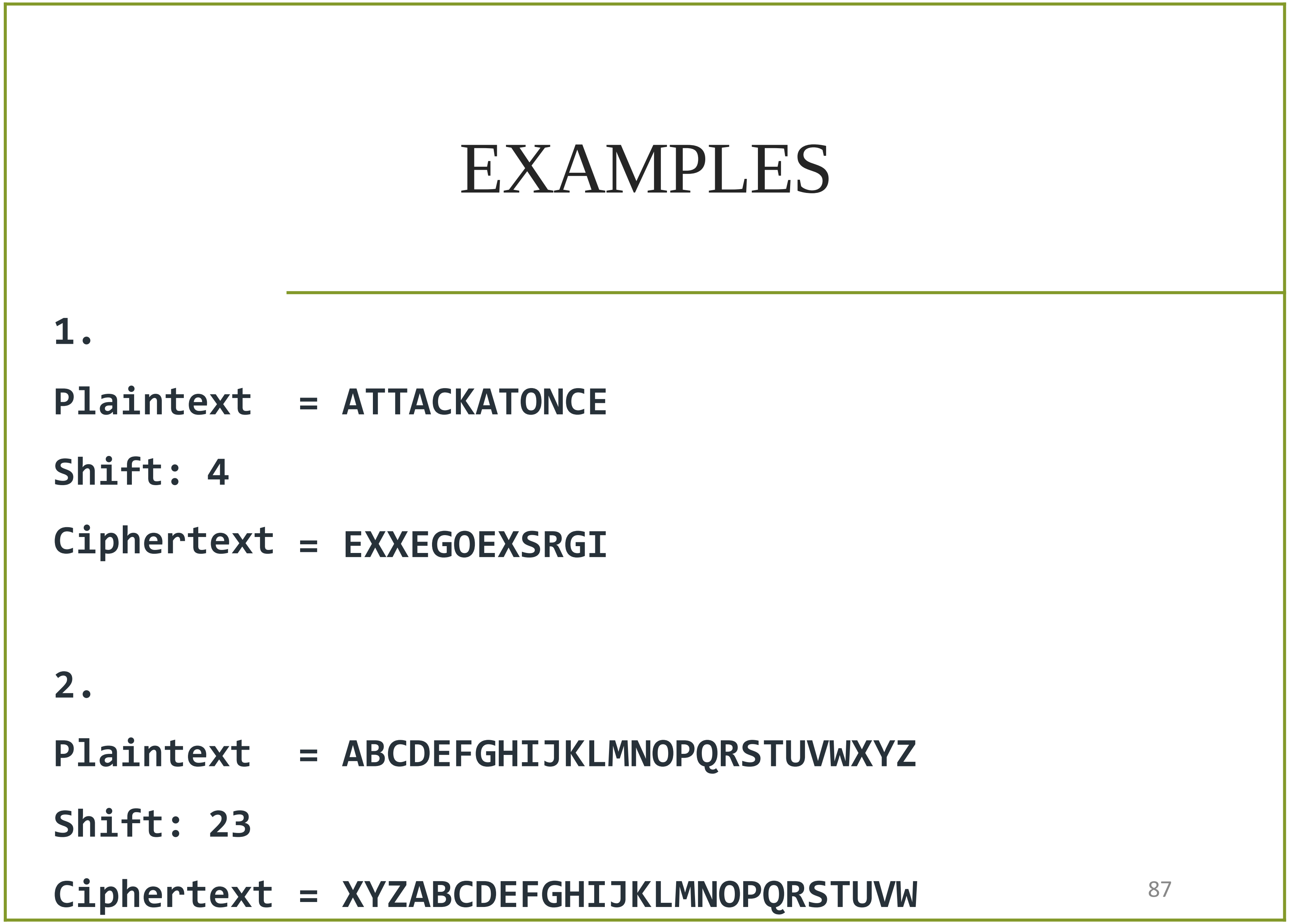
- The Caesar cipher shifts all the letters in a piece of text by a certain number of places. The key for this cipher is a letter which represents the number of place for the shift.
- A key D means “shift 3 places” and a key M means “shift 12 places”.
- Note that a key A means “do not shift” and a key Z can either mean “shift 25 places” or “shift one place backwards”.
- The following cipher alphabet is generated from shifting by X (i.e. 23)



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	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



```
Plaintext:  THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Ciphertext: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD
```



EXAMPLES

1.

Plaintext = ATTACKATONCE

Shift: 4

Ciphertext = EXXEGOEXSRGI

2.

Plaintext = ABCDEFGHIJKLMNOPQRSTUVWXYZ

Shift: 23

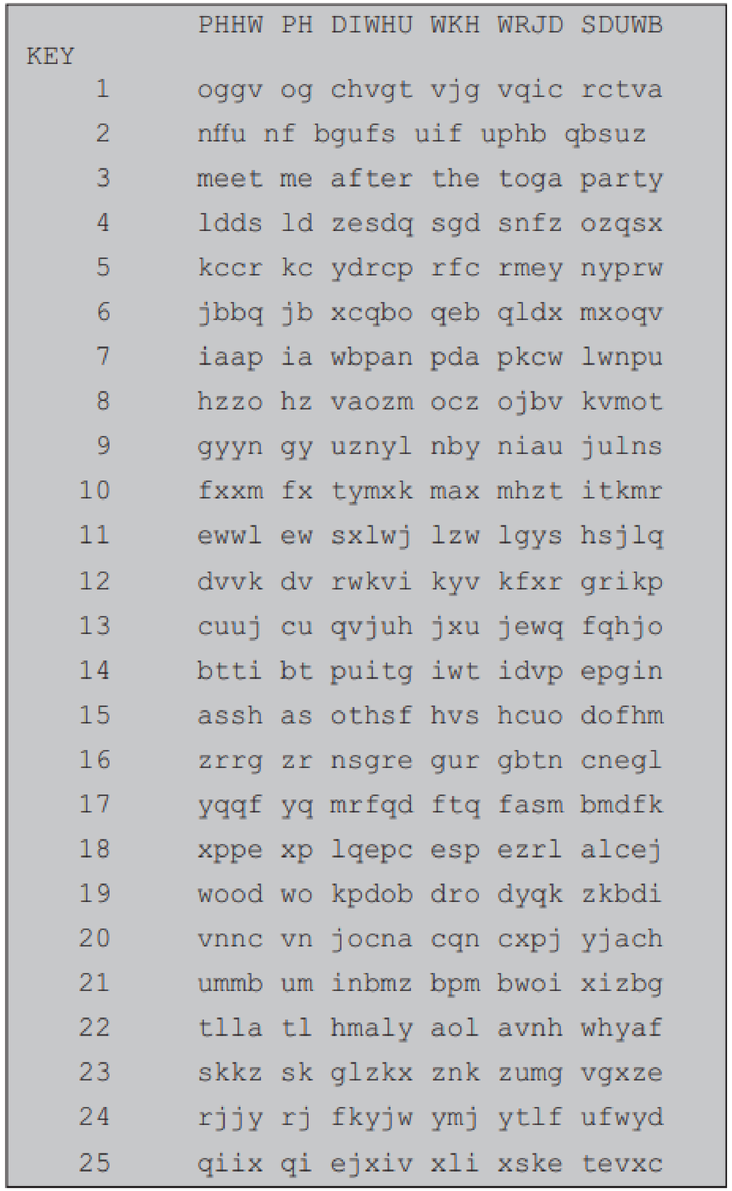
Ciphertext = XYZABCDEFGHIJKLMNOPQRSTUVW

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. In this case, the plaintext leaps out as occupying the third line. 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.



```
           PHHW PH DIWHU WKH WRJD SDUWB
KEY
     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 ydrcp rfc 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 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 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 glzkx znk zumg vgxze
    24     rjjy rj fkyjw ymj ytlf ufwyd
    25     qiix qi ejxiv xli xske tevxc
```

Brute-Force Cryptanalysis of Caesar Cipher

AFFINE CIPHER

The **affine cipher** is a type of monoalphabetic substitution cipher , where each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter.

- The Affine has two numbers in its key: a **multiplier** and a **shift size**.
- Both of **a** and **b** must have no factors in common with module **m**. For example 15 and 26 have no factors in common, so 15 is an acceptable value for *a*, however 12 and 26 have factors in common (e.g. 2) so 12 cannot be used for value of *a*.

- To encrypt and decrypt with affine algorithm , we first convert all the letters to numbers ('a'=0, 'b'=1, ..., 'z'=25) then use the following equations to calculate and find the ciphertext:

To encrypt: $\mathrm{E}(x) = (ax + b) \bmod m,$

To decrypt: $\mathrm{D}(x) = a^{-1}(x - b) \bmod m,$

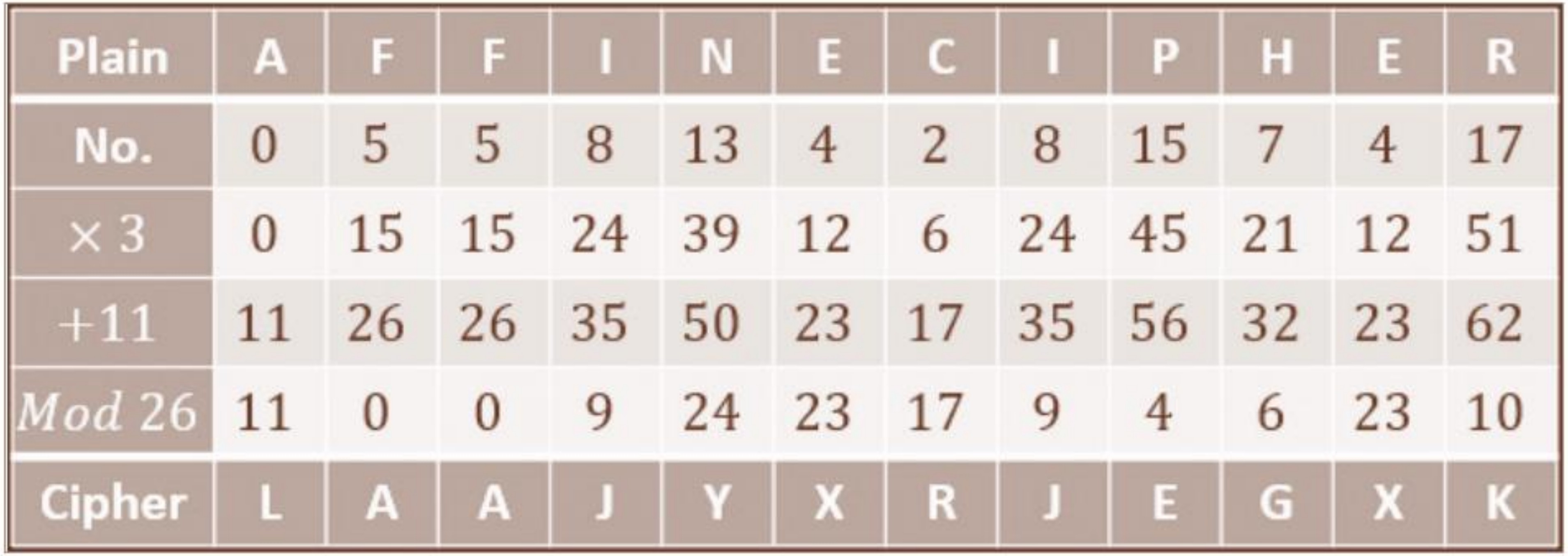
Where $1 = aa^{-1} \bmod m.$

a^{-1} is the multiplicative inverse of *a*

AFFINE CIPHER

Here is an example to see how the two parts in an Affine cipher key are used. We will encrypt **'affine cipher'** using a multiplier of 3 followed by a shift of 11:

The solution : P=“affine cipher a=3 , b=11



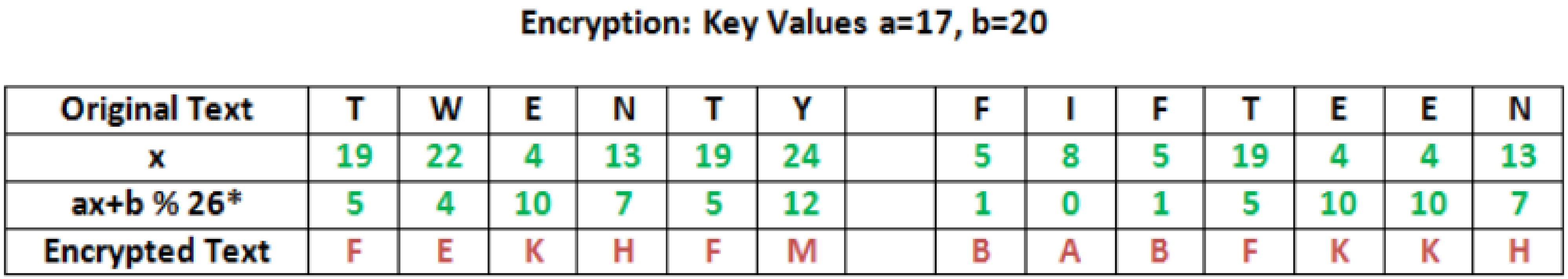
Plain	A	F	F	I	N	E	C	I	P	H	E	R
No.	0	5	5	8	13	4	2	8	15	7	4	17
× 3	0	15	15	24	39	12	6	24	45	21	12	51
+11	11	26	26	35	50	23	17	35	56	32	23	62
Mod 26	11	0	0	9	24	23	17	9	4	6	23	10
Cipher	L	A	A	J	Y	X	R	J	E	G	X	K

H.W.

Decrypt the above ciphertext (note that 3^{-1} in mod 26) = 9

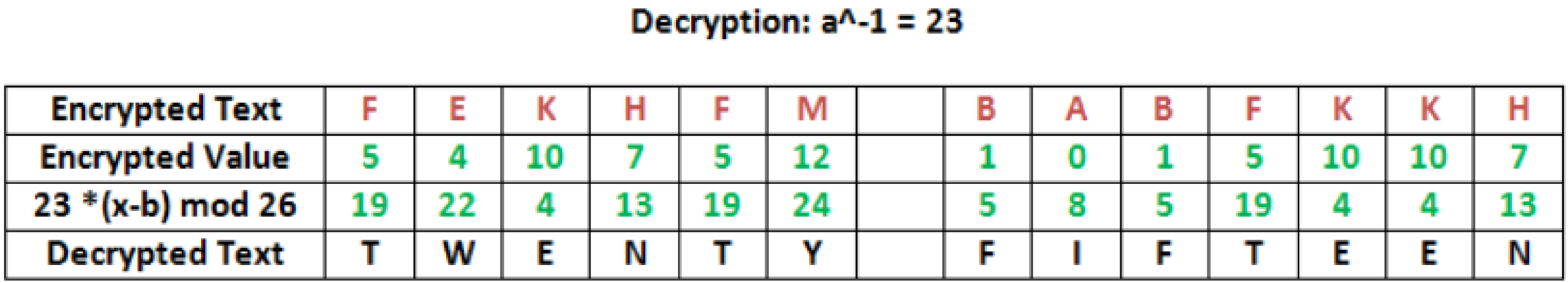
Example:

Plaintext = twenty fifteen, multiplier =17 and shift by 20



Encryption: Key Values a=17, b=20

Original Text	T	W	E	N	T	Y		F	I	F	T	E	E	N
x	19	22	4	13	19	24		5	8	5	19	4	4	13
ax+b % 26*	5	4	10	7	5	12		1	0	1	5	10	10	7
Encrypted Text	F	E	K	H	F	M		B	A	B	F	K	K	H



Decryption: a^-1 = 23

Encrypted Text	F	E	K	H	F	M		B	A	B	F	K	K	H
Encrypted Value	5	4	10	7	5	12		1	0	1	5	10	10	7
23 *(x-b) mod 26	19	22	4	13	19	24		5	8	5	19	4	4	13
Decrypted Text	T	W	E	N	T	Y		F	I	F	T	E	E	N

Note: If any negative value is appeared in the decryption process, add 26 to the result and continue.

VIGENÈRE CIPHER

The **Vigenère cipher** (First described in 1553),is a method of encrypting alphabetic text by using a series of interleaved Caesar ciphers, based on the letters of a keyword. It employs a form of **polyalphabetic substitution**

The best known, and one of the simplest, polyalphabetic ciphers is the Vigenère cipher. In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter, which is the ciphertext letter that substitutes for the plaintext letter a. Thus, a Caesar cipher with a shift of 3 is denoted by the key value 3.

To encrypt a message, a key is needed that is as long as the message. Usually, the key is a **repeating keyword.**

A general equation of the encryption process is

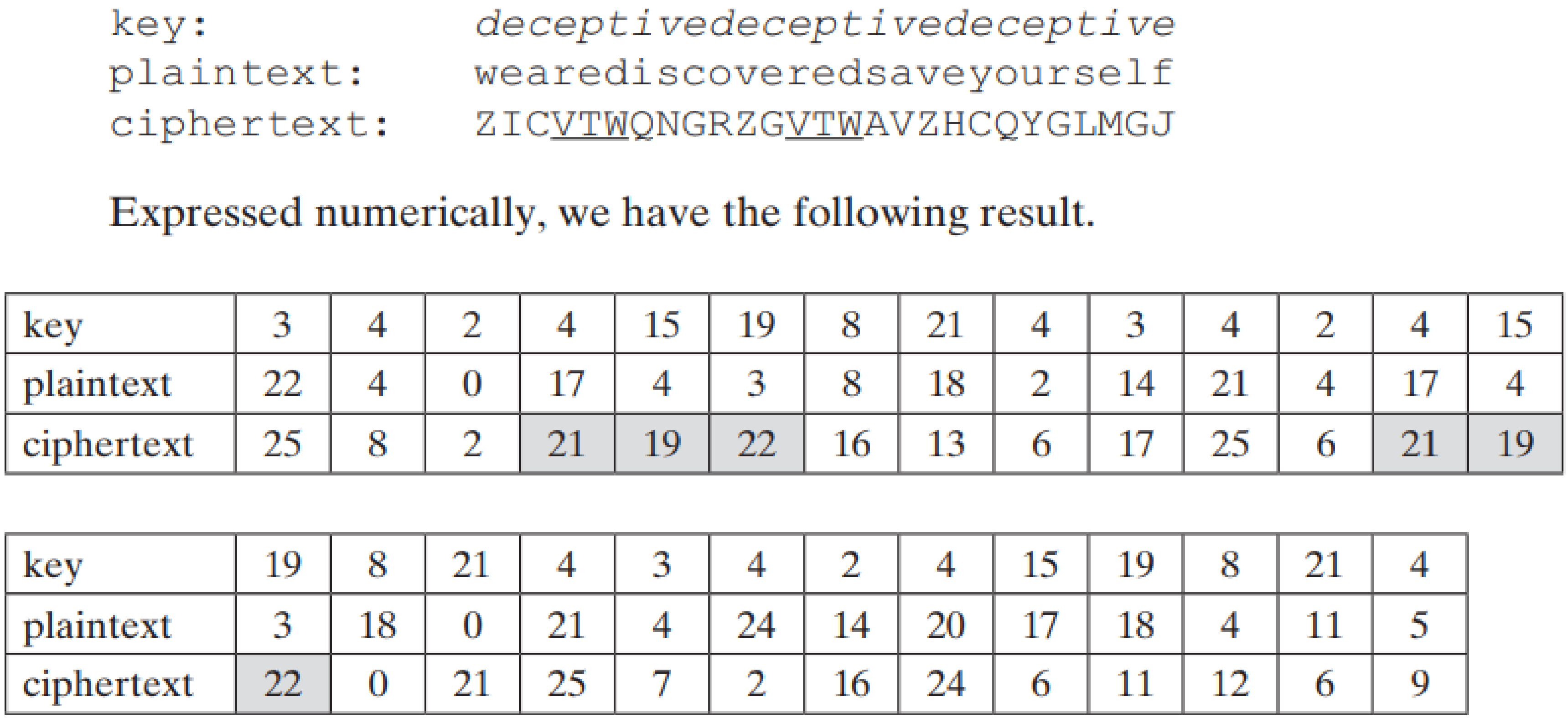
$$\mathbf{Ci = (pi + ki \bmod m) \bmod 26}$$

Similarly, decryption is a generalization of Equation :

$$\mathbf{pi = (Ci - ki \bmod m) \bmod 26}$$

Example (1)

Use **Vigenère** cipher algorithm to encrypt the message "**we are discovered save yourself**" if the keyword is (**deceptive),**



```
key:          deceptivedeceptivedeceptive
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Expressed numerically, we have the following result.

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

NOTE:

The **strength** of this cipher is that there are multiple ciphertext letters for each plaintext letter, one for each unique letter of the keyword. Thus, the letter frequency information is obscured.

But this cipher suffers from duplicating the ciphertext when the plaintext and the key are similar.

Example 2: (using Vigenère table)

Plaintext : hello how are you
Keyword: green

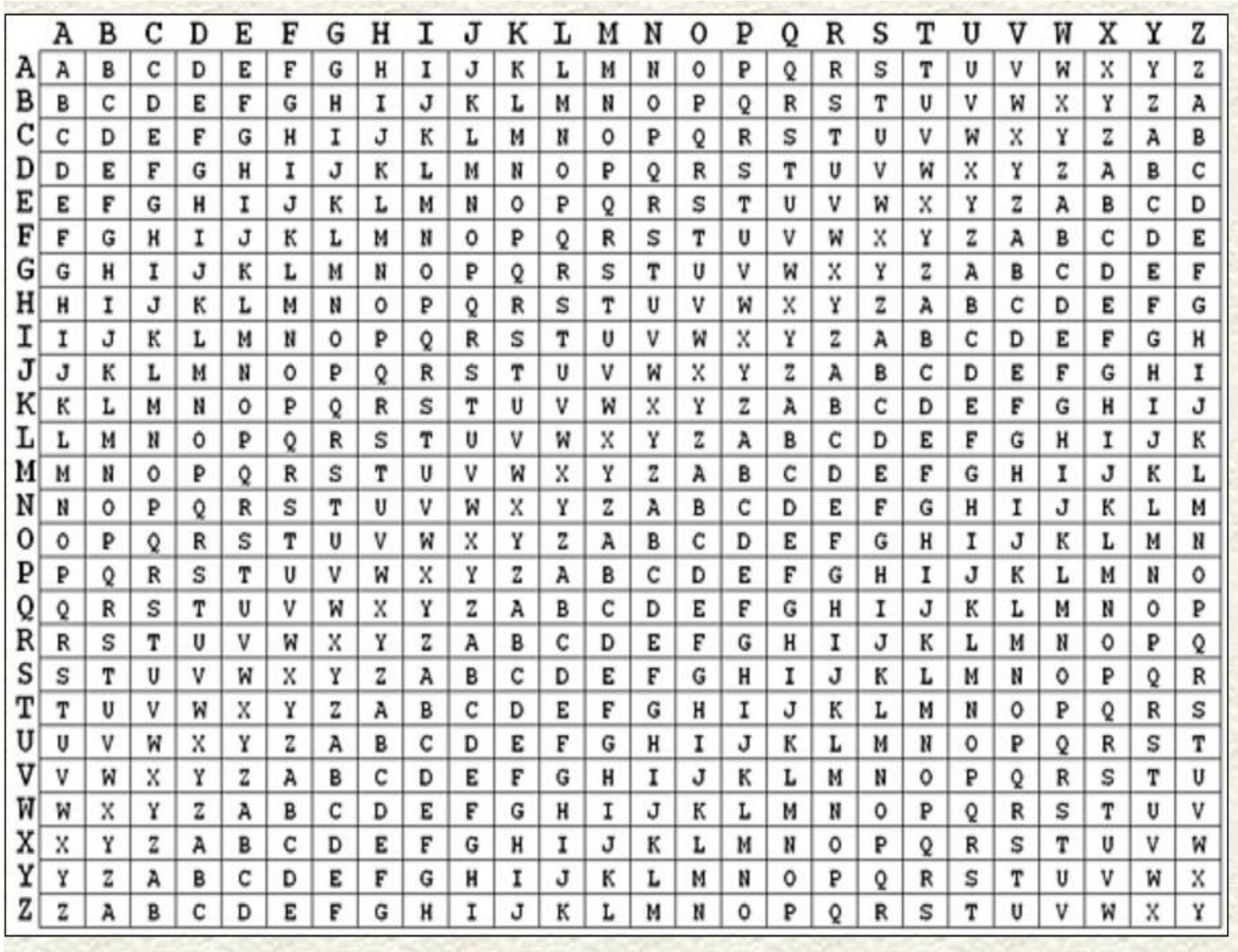
Keyword	GREENGREENGREE
Plaintext	hellohowareyou
Ciphertext	NVPPBNFAEEKPSY

H.W.

Solve the same problem using the equations approach

key

plaintext



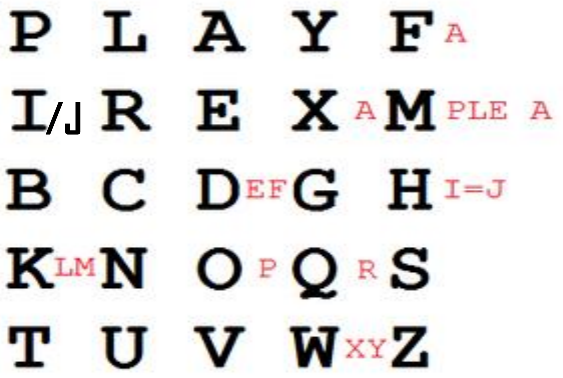
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

PLAYFAIR CIPHER (or PLAYFAR SEQUARE)

- It is the best-known **multiple-letter encryption cipher** (also known as **Polygram cipher systems (or polygraphic ciphers)**
- **Polygraphic substitution** is a cipher in which a uniform substitution is performed on blocks of letters. When the length of the block is specifically known, more precise terms are used: for instance, a cipher in which pairs of letters are substituted is **bigraphic**.

- It was invented in **1854**, and treats diagrams in the plaintext as single units and translates these units into ciphertext diagrams
- The Playfair algorithm is based on the use of **a 5 * 5 matrix of letters** constructed using a keyword. Here is an **example,**

The keyword is "**Playfair example**"

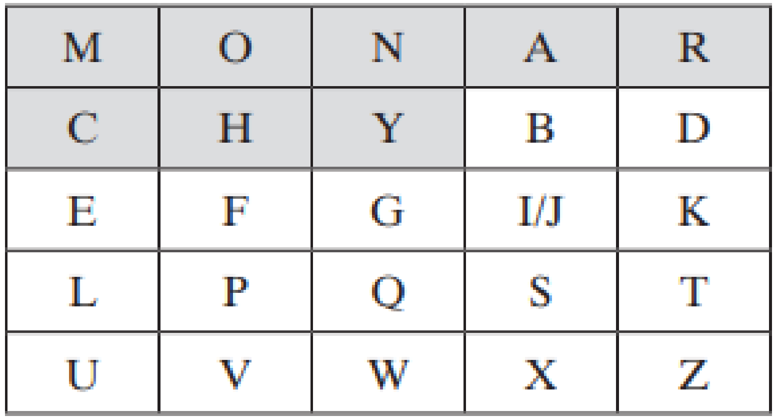


P	L	A	Y	F
I/J	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

A
A
PLE A
EF
I=J
LM
P
R
XY

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.

Playfair Cipher: How to encrypt



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

The keyword is **monarchy.**

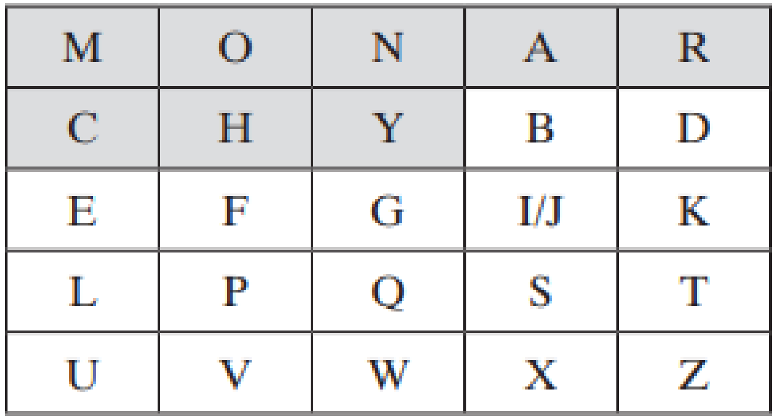
Steps to encrypt a plaintext:

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 under, 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 need).

To decrypt any ciphertext the reversal steps are implemented.

To encrypt the message (balloon) with 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

1. Plaintext blocks will be
   ba lx lo on

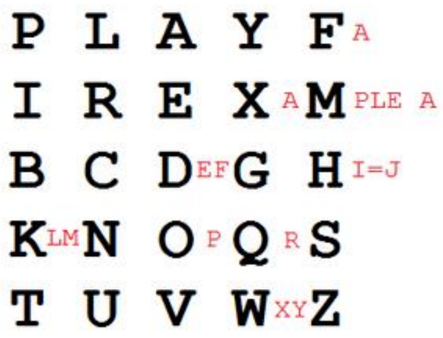
Ba➔	**Ib**
Lx➔	**Su**
Lo➔	**Pm**
On➔	**Na**

Ciphertext = **ipsupmna**

Example 1:

Use Playfair algorithm to encrypt the message "hide the gold in the tree stump“ using the keyword : Playfair example”

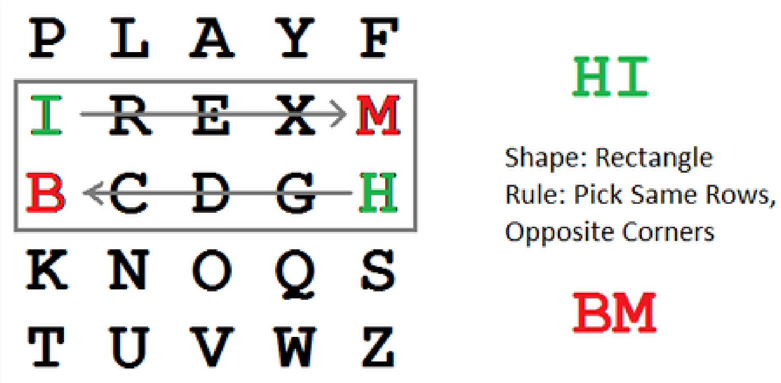
The Playfair matrix



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

The solution :

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



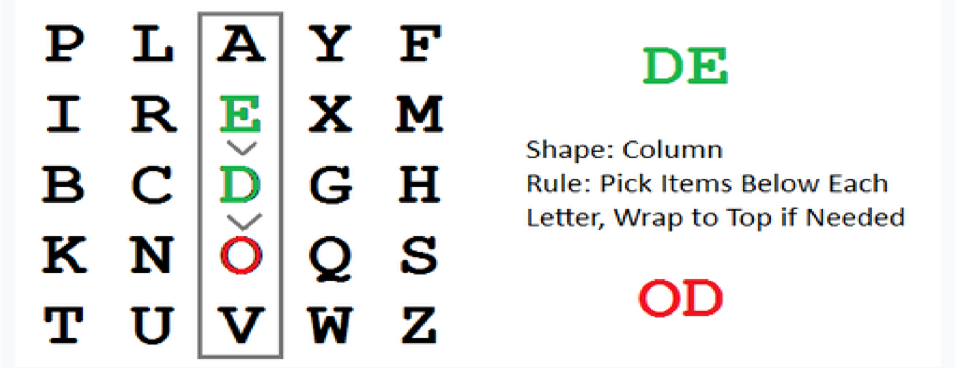
P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

HI

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

BM

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



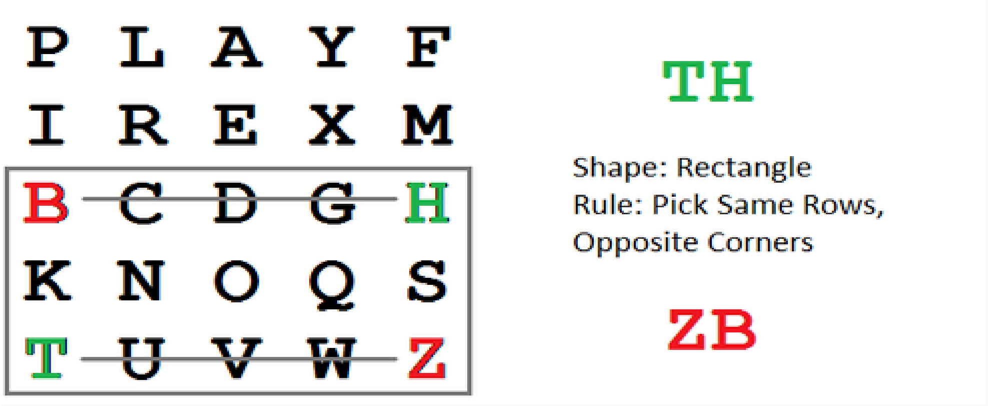
P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

DE

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

OD

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



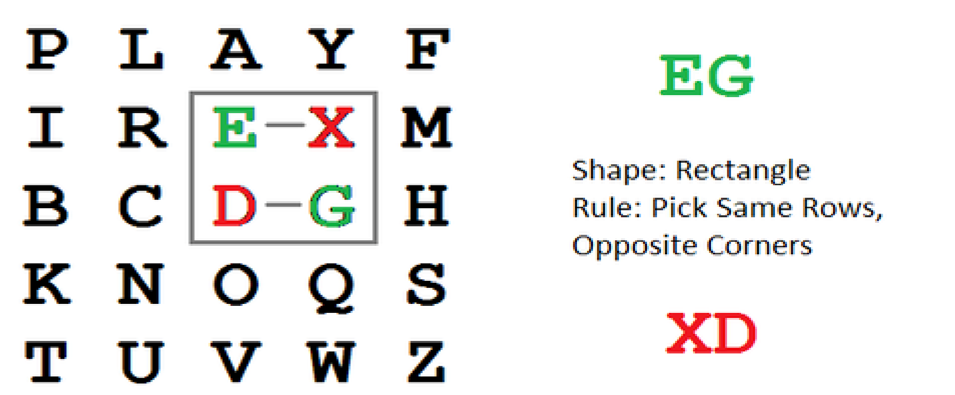
P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

TH

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

ZB

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

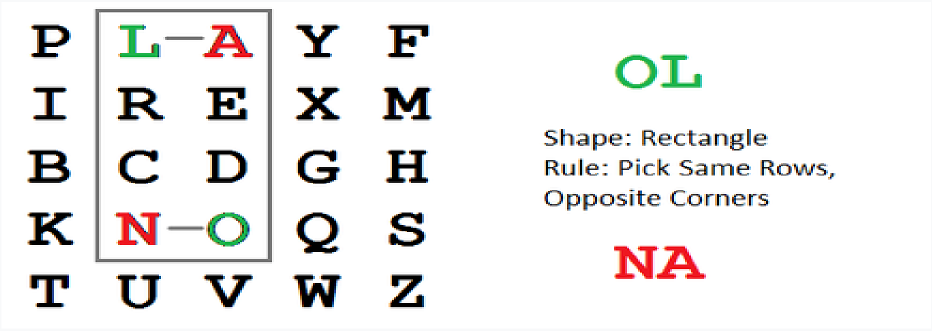
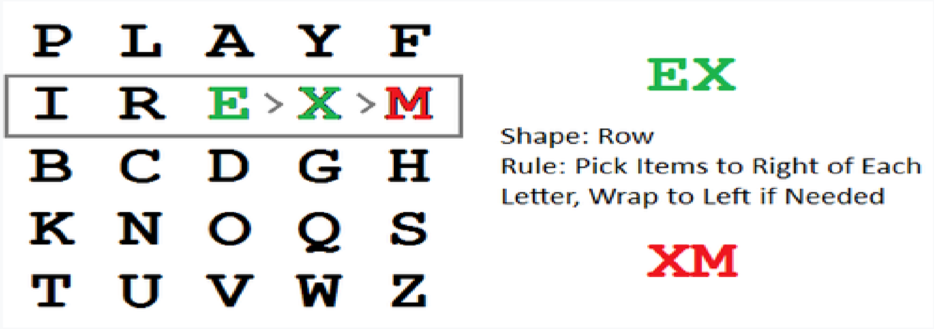


P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

EG

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

XD

5. The pair OL forms a rectangle, replace it with NA	 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 OL Shape: Rectangle Rule: Pick Same Rows, Opposite Corners NA
6. The pair DI forms a rectangle, replace it with BE	
7. The pair NT forms a rectangle, replace it with KU	
8. The pair HE forms a rectangle, replace it with DM	
9. The pair TR forms a rectangle, replace it with UI	
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
11. The pair ES forms a rectangle, replace it with MO	
12. The pair TU is in a row, replace it with UV	
13. The pair MP forms a rectangle, replace it with IF	

H.W.

1. Decrypt all example of Playfair algorithm
2. Encrypt and decrypt the message “instruments" by keyword : **monarchy**.

HILL CIPHER

- In classical cryptography, the **Hill cipher** is a **polygraphic substitution cipher** based on **linear algebra**.
- Invented by Lester S. Hill in 1929.

- To encrypt a message, each block of *n* letters (considered as an *n*-component vector) is multiplied by an invertible *n* × *n* matrix, against modulus 26.
- To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.
- The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of **invertible *n* × *n* matrices** (modulo 26).

HILL CIPHER:

Example 1:

Use Hill cipher algorithm to encrypt the message "mp" using the key matrix ($\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$ (or $\begin{pmatrix} h & i \\ l & l \end{pmatrix}$ or we can say that the key $=$ "$\boldsymbol{hill}$" if you know that the encryption process take each two char together)

Solution:

Plaintext="mp" $=\begin{pmatrix} 12 \\ 15 \end{pmatrix}$

Ciphertext = $\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 12 \\ 15 \end{pmatrix}$

7*12 + 8*15 =204

11*12 + 11*15 =297

H.W.

P=send

Key= $\begin{pmatrix} \mathbf{7} & \mathbf{8} \\ \mathbf{11} & \mathbf{11} \end{pmatrix}$

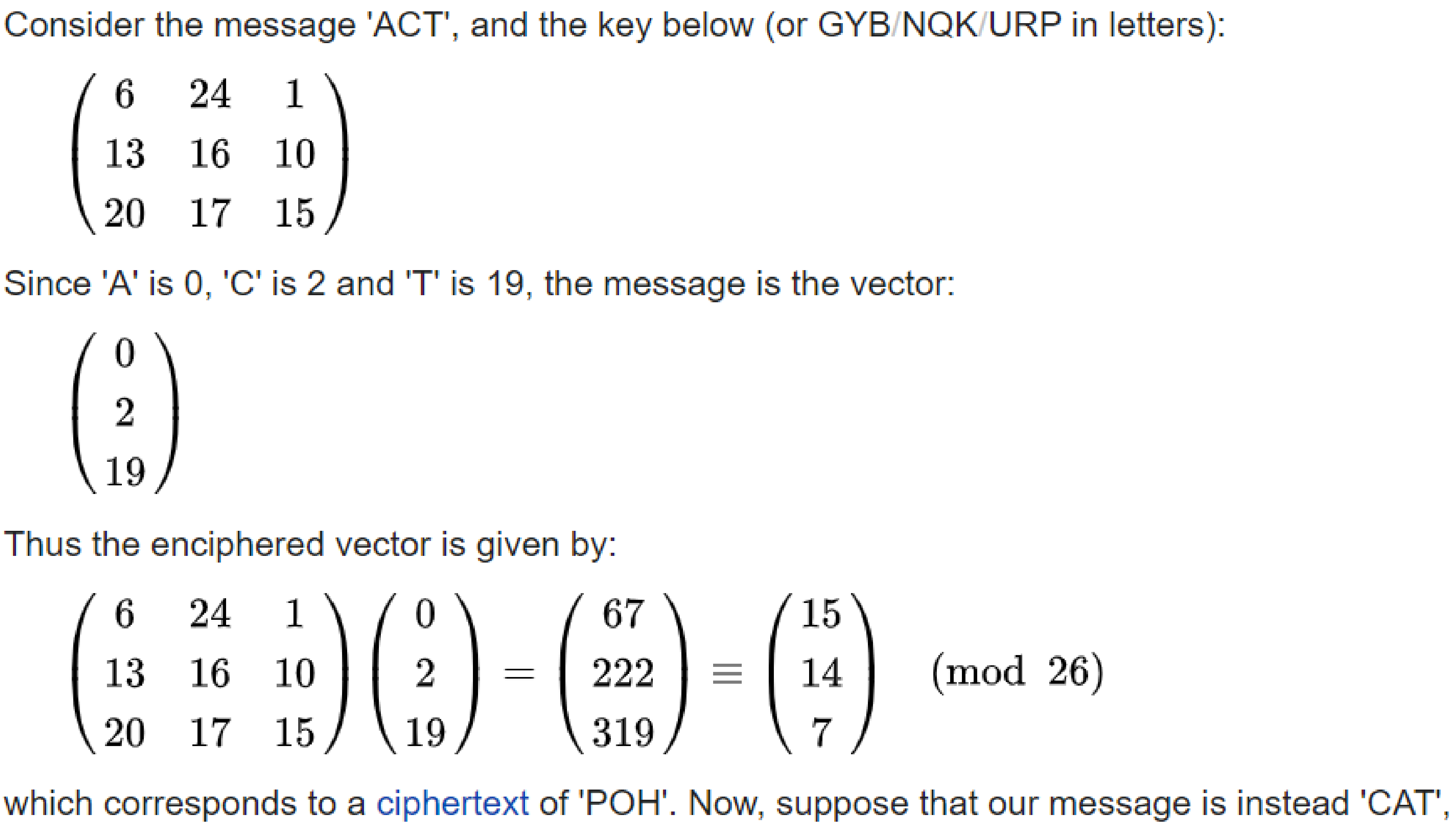
So

Ciphertext = $\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 12 \\ 15 \end{pmatrix}$ = $\begin{pmatrix} 204 \\ 297 \end{pmatrix}$ mod 26

= $\begin{pmatrix} 22 \\ 11 \end{pmatrix}$ ➔ $\begin{pmatrix} w \\ l \end{pmatrix}$

so the final ciphertext is : "wl"

Example 2:



Consider the message 'ACT', and the key below (or GYB/NQK/URP in letters):

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

Since 'A' is 0, 'C' is 2 and 'T' is 19, the message is the vector:

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

Thus the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

which corresponds to a ciphertext of 'POH'. Now, suppose that our message is instead 'CAT',

What is the output ciphertext? → H.W.