Chapter Two
CRYPTOGRAPHY

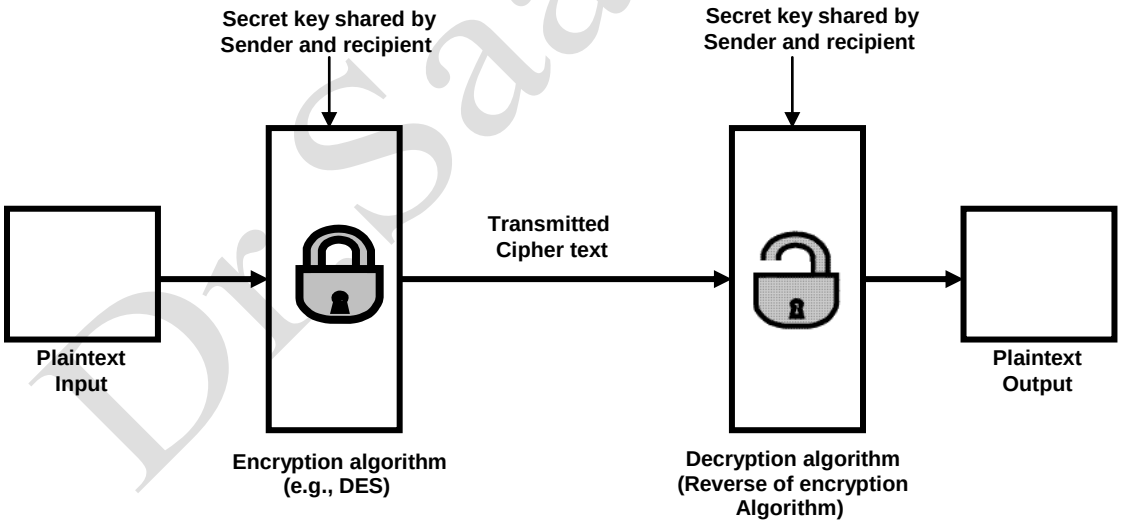
Introduction

A cryptographic algorithm, or cipher, is a mathematical function used in encryption and decryption processes. A cryptographic algorithm works in combination with a key- (word, number, or phrase) to encrypt the plaintext.

Cryptosystem (Cryptographic System) is clarified by the following transformation diagram:

$$M \xrightarrow{F} C \xrightarrow{F^{-1}} M$$

Were M the set of all possible plaintext, C the set of all possible cipher text and F is a 1 – to – 1 correspondence, this means given a cipher text unit, there is one and only one plaintext message unit for which it is the encryption.



Encryption / Decryption Algorithm for Conventional systems

Examples for Cryptosystem are : DES, 3DES, IDEA, RSA, ElGamal, PGP, etc. The original form of a message is known as a plain text and the encrypted form is called a cipher text.

The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. A Cryptographic algorithm, plus all possible keys and all the protocols that make it work, comprise a cryptosystem or encryption scheme.

Cryptography is the science of constructing of cryptosystem.

Cryptology is the science of Cryptography and Cryptanalysis.

Cryptanalysis is the science of mathematical techniques to break cryptosystem.

Steganography is the science / art of hiding information inside objects.

Cryptography can be understood as **Crypt = Secret** and **Graph = writing**

Steganography can be understood as **Stega=hidden** and **Graph= writing**

Examples:

Hiding message in a text file.
Hiding copyright mark in an image file.
Hiding message in a picture.
Hiding sound in picture.

Traditionally, cryptography was used mainly for military and Diplomatic purposes , however, in recent years the actual and potential applications of cryptosystems of cryptography have expanded to include many other areas where communication systems play a vital role – collecting and keeping records of confidential data, electronic financial transactions, and so on.

A cryptanalyst's task is to **break** an encryption, this means that the cryptanalyst attempts to deduce the meaning of a cipher text message, or to determine a decrypting algorithm that matches an encrypting algorithm.

SYMMETRIC CIPHER MODEL:

The components of cryptosystem for a symmetric encryption scheme :

1- **Plaintext**:This is the original intelligible message or data that is fed into the algorithm as input.
2- Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.

3- **Secret key**: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

4- **Cipher text**: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher text.

5- **Decryption algorithm**:This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

There are two requirements for secure use of conventional encryption:

1- We need a strong encryption algorithm. The opponent must be unable to decipher the cipher text or figure out the key even if he or she is in possession of a number of cipher texts together with the plaintext that produced each cipher text.

2- Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

Cryptographic systems are characterized along three independent dimensions:

1- The type of operations used for transforming plaintext to cipher text. All encryption algorithms are used on two general principals:

Substitution in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which each element in the plaintext are rearranged. The fundamental requirement is no information be lost (that is, all operations are reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and **transpositions**.

2- The number of keys used: If both sender and receiver use the same keys, the system is referred to as symmetric, single-key, secret key, or conventional encryption. If the sender and receiver each uses a different key, the system is referred to as asymmetric two key, or public-key encryption.

3- The way in which the plaintext is processed.

A **block** cipher processes the input one block of elements at a time, producing an output block for each input block.
A **stream** cipher processes the input elements continuously producing output one element at a time, as it goes along.

CRYPTANALYSIS:

There are two general approaches to attacking a conventional encryption scheme:

A- Cryptanalysis

Cryptanalytic attack rely on the nature of the algorithm plus perhaps some knowledge of the general characters of the plaintext or even some sample plaintext cipher text pairs.

This type of attacks exploits the characteristics of the algorithm to attempt to reduce a specific plaintext or to deduce the key being used. If the attack succeeds

in deducing the key, the effect is catastrophic, {All future and past messages encrypted with that key are compromised.

B- Brute-force attack:

The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

Classification of cipher systems

A-Secret key system

1- Conventional systems(classic)

a- Transposition cipher

I- Simple

1- Message reversal cipher

2- Columnar transposition

II-Double

b-Substitution cipher

i- Monoalphabetic

1- Simple

a-Direct stander

b- Standard reverse

c- Multiplicative cipher

d- Affine cipher

e- Mixed cipher

f- Key word mixed

g- Transposed keyword mixed

ii- Homophonic

a-Vigenere

b-Beaufort

iii-Poygraphic

a-Playfair

b-Hill cipher

2-Modren systems

a- Block cipher

1- DES (Data Encryption standards).

b-Stream cipher

1- LFSR(linear feedback Shift Register)

ii-Public key systems

1-RSA

Transposition cipher

Plain text → arrange in different order → cipher text

1- Message reversal cipher

Encryption

Ex:

Plain text = ALMAMON UNVERSITY COLLEGE

Cipher text=EGELLOCYTISREVNUNOMAMLA

2- Columnar Transposition

1- Arrange the message as array of two dimensional .

2- The number of row and column depends on length of message

3- If length of message is 30 then the number of rows and columns are :
15x2 , 2 x15 ,10x3 ,3 x10,5x6,6x5
Note : if the length of message =29 then add number one character
Encryption algorithm

1- Broadcast the message as row

2- Arrange the columns respect to key

3- Write the cipher text as column

Ex:

Key = (2,3,1)

Message = ALMAMOON UNIVERSITY COLLEGE

1	2	3
A	L	M
A	M	O
O	N	U
N	I	V
E	R	S
I	T	Y
C	O	L
L	E	G
E	X	X

2	3	1
L	M	A
M	O	A
N	U	O
I	V	N
R	S	E
T	Y	I
O	L	C
E	G	L
X	X	E

Cipher text =LMNIRTOEX/MOUVSYLGX/AAONEICLE

Decryption

1- Broadcast the cipher text as column respect to key
2- Arrange the key with ascending order with its column
3- Write the plain text as row

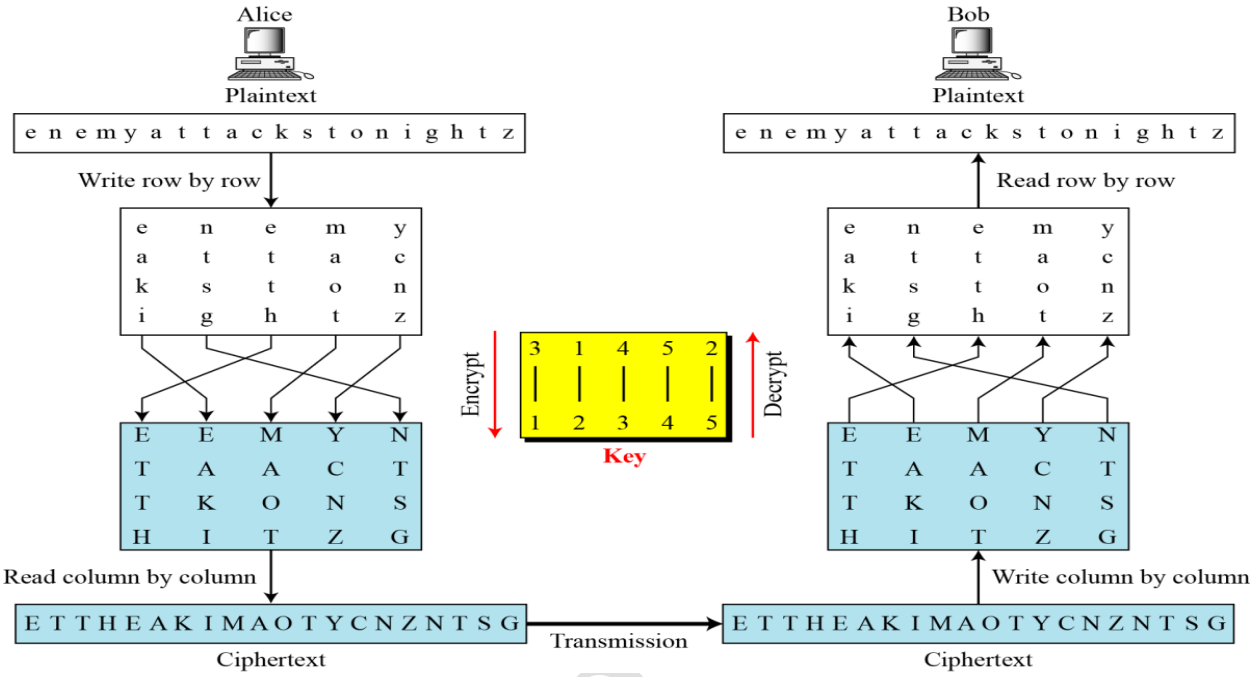
2	3	1
L	M	A
M	O	A
N	U	O
I	V	N
R	S	E
T	Y	I
O	L	C
E	G	L
X	X	E

2-Arrange the key

1	2	3
A	L	M
A	M	O
O	N	U
N	I	V
E	R	S
I	T	Y
C	O	L
L	E	G
E	X	X

Plain text = ALMAMOONUNIVERSITYCOLLEGE

Note : We can take a keyword like "USE"



encryption Algorithm

Plane text :- the two application may use the same key for each of two steps.

1- Pick the keyword ,such as “DESCRIBE”
2- Write the plane text under it in rows
3- Number the letters in the keyword in alphabetical order
4- Read the cipher off by columns

Ex

Plain text=THE TWO APLICATION MAY USE THE SAME KEY FOR EACH OF THE TWO STEPS

KEY =DESCRIBE

KEY=BCDEEIRS

B=1 C=2 D=3 E=4 E=5 I=6 R=7 S=8

D	E	S	C	R	I	B	E
T	H	E	T	W	O	A	P
P	L	I	C	A	T	I	O
N	M	A	Y	U	S	E	T
H	E	S	A	M	E	K	E

Y	**F**	**O**	**R**	**E**	**A**	**C**	**H**
O	**F**	**T**	**H**	**E**	**T**	**W**	**O**
S	**T**	**E**	**P**	**S**	**X**	**X**	**X**

3	**4**	**8**	**2**	**7**	**6**	**1**	**5**
D	**E**	**S**	**C**	**R**	**I**	**B**	**E**
T	**H**	**E**	**T**	**W**	**O**	**A**	**P**
P	**L**	**I**	**C**	**A**	**T**	**I**	**O**
N	**M**	**A**	**Y**	**U**	**S**	**E**	**T**
H	**E**	**S**	**A**	**M**	**E**	**K**	**E**
Y	**F**	**O**	**R**	**E**	**A**	**C**	**H**
O	**F**	**T**	**H**	**E**	**T**	**W**	**O**
S	**T**	**E**	**P**	**S**	**X**	**X**	**X**

CIPHER TEXT =

AIEKCWX/TVYARHP/TPNHYOS/HLMEFFT/POTEHOX/OTSEATX/WAUMEES/EIASOTE

Decryption

1- Construct a block with right number of rows under the keyword.

2- Blocking off the short columns

3- Write The cipher in by columns

3	4	8	2	7	6	1	5
D	**E**	**S**	**C**	**R**	**I**	**B**	**E**
T	**H**	**E**	**T**	**W**	**O**	**A**	**P**
P	**L**	**I**	**C**	**A**	**T**	**I**	**O**
N	**M**	**A**	**Y**	**U**	**S**	**E**	**T**
H	**E**	**S**	**A**	**M**	**E**	**K**	**E**
Y	**F**	**O**	**R**	**E**	**A**	**C**	**H**
O	**F**	**T**	**H**	**E**	**T**	**W**	**O**
S	**T**	**E**	**P**	**S**	**X**	**X**	**X**

D	**E**	**S**	**C**	**R**	**I**	**B**	**E**

T	**H**	**E**	**T**	**W**	**O**	**A**	**P**
P	**L**	**I**	**C**	**A**	**T**	**I**	**O**
N	**M**	**A**	**Y**	**U**	**S**	**E**	**T**
H	**E**	**S**	**A**	**M**	**E**	**K**	**E**
Y	**F**	**O**	**R**	**E**	**A**	**C**	**H**
O	**F**	**T**	**H**	**E**	**T**	**W**	**O**
S	**T**	**E**	**P**	**S**	**X**	**X**	**X**

Plain text = **THE TWO APPLICATION MAY USE THE SAME KEY FOR EACH OF TWO STEPS**

Using Matrices

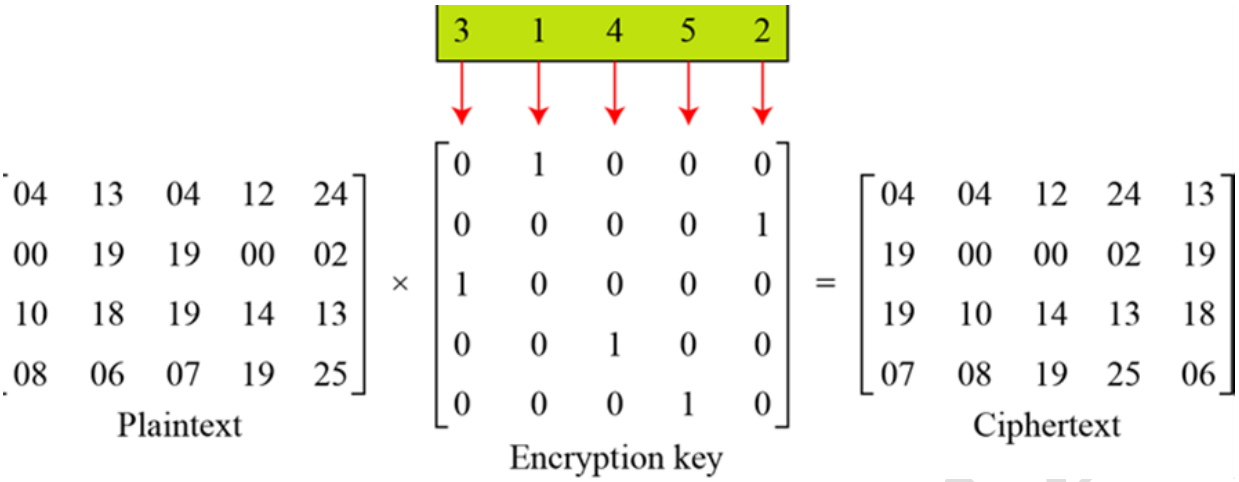
We can use matrices to show the encryption/decryption process for a transposition cipher.

Example

Figure down shows the encryption process. Multiplying the 4 × 5 plaintext matrix by the 5 × 5 encryption key gives the 4 × 5 ciphertext matrix

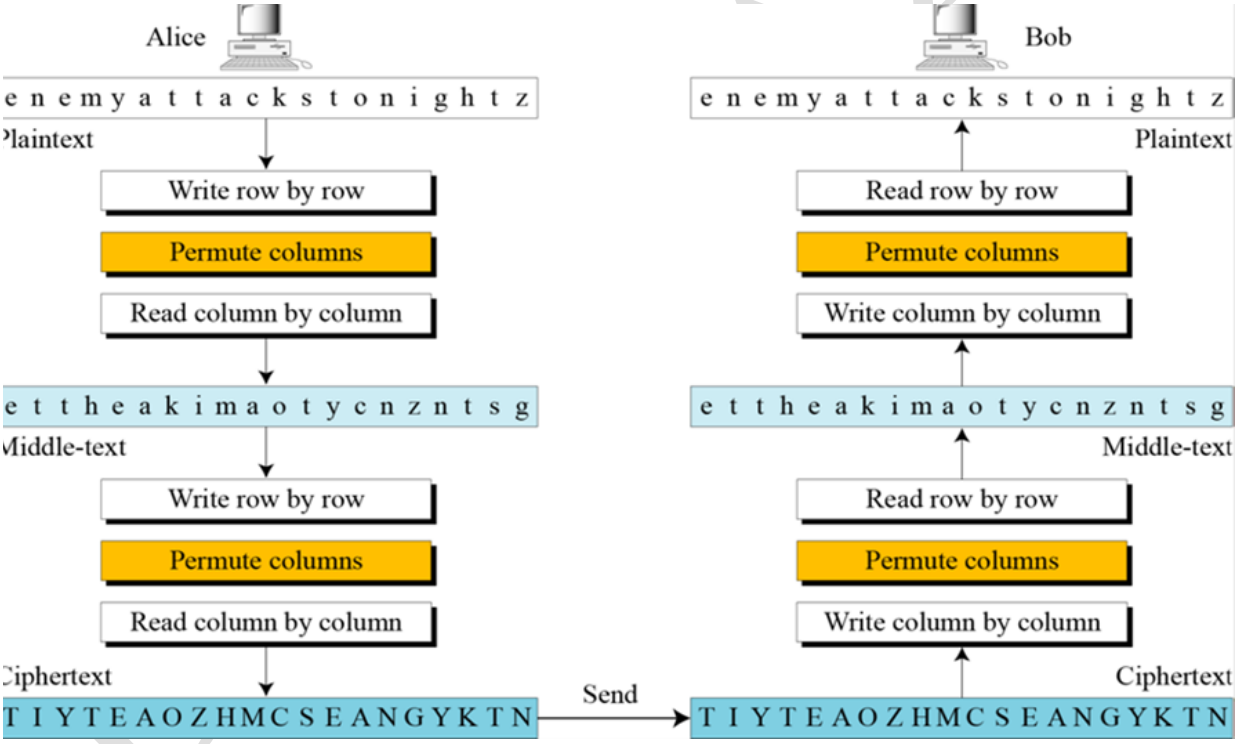
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

19	20	21	22	23	24	25
T	U	V	W	X	Y	Z



I-Double

Double Transposition Ciphers



Direct standard alphabet or Caesar Cipher:

The earliest known use of a substitution cipher, and simplest, was by Julius Caesar:

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

For example:

Plain:	meet	me	after	the	toga	party
Cipher:	PHHW	PH	DIWHU	WHK	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
Key = 4

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 cipher text letter
C= E(p) = {p+3} mod (26)

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

$C=E_k(p) = (p+k) \bmod 26$
$P= D_k (c) = (c-k) \bmod 26$
K is the key

Ex1 : Encrypt the Plain text = THIS using direct standard alphabet with KEY = 3 ?

T= 19 H= 7 I=8 S=18
$E_k(T) = (T+KEY) \bmod 26 = (19 + 3) \bmod 26 = 22 \bmod 26 = 22 \rightarrow W$
$E_k(H) = (H+KEY) \bmod 26 = (7 + 3) \bmod 26 = 10 \bmod 26 = 10 \rightarrow K$
$E_k(I) = (I+KEY) \bmod 26 = (8 + 3) \bmod 26 = 11 \bmod 26 = 11 \rightarrow L$
$E_k(S) = (S+KEY) \bmod 26 = (18 + 3) \bmod 26 = 21 \bmod 26 = 21 \rightarrow V$

Cipher text = WKLV

Ex1 : Decrypt cipher text = WKLV using direct standard alphabet with KEY = 3 ?

Ex :Decryption

$D_K(W)$ =(W-KEY) mod 26 = (22-3) mod 26 = 19 mod 26 = 19 →T
$D_K(K)$ =(K-KEY) mod 26 = (10-3) mod 26 = 7 mod 26 = 7 →H
$D_K(L)$ =(L-KEY) mod 26 = (11 - 3) mod 26 = 11 mod 26 = 11 →I
$D_K(V)$ =(V-KEY) mod 26 = (21-3) mod 26 = 18 mod 26 = 18 → S

Plain text = THIS

Note
Find -10 mod 26
a + 10 mod 26 = 0
a= 16

EX 2 : **Ex1 : Encrypt the** Plain text =" TQ " using direct standard alphabet with KEY = 12 ?

$E_k(T)$ = (T+KEY) mod 26 = (19 + 12) mod 26 = 31 mod 26 =5 → F
$E_k(Q)$ = (Q+KEY) mod 26 = (16 + 12) mod 26 = 28 mod 26 =2 → C

$D_K(F)$ =(F-KEY) mod 26 = (5-12) mod 26 = -7 mod 26 = 19 →T
$D_K(C)$ =(C-KEY) mod 26 = (2-12) mod 26 = -10 mod 26 = 16 →Q

31=1*26 + 5
-7 mod 26 = 26-7=19

2- Multiplicative cipher

Cipher based on multiply each character by a key k
$E_k(m)$ =(m*k) mod 26
i.e odd number and not equal to 13

Ex: Encryption

K=9
Plain text = ALMAMON UNIVERSITY
$E_K(m) = (m*k) \bmod 26$
$E_9(A) = (0*9) \bmod 26 = 0 = A$
$E_9(L) = (11*9) \bmod 26 = 99 \bmod 26 = 21 = V$
$E_9(M) = (12*9) \bmod 26 = 108 \text{ MOD } 26 = 4 = E$

Cipher text = "AVEAEWNYNHKXGUPI"

99- 26 * 3=21

Ex: Encryption

$K^{-1} = 3$

Cipher text = AVE

$D_K(p) = (p*k^{-1}) \bmod 26$

$D_9(A) = (0*3) \bmod 26 = 0 = A$

$D_9(V) = (21*3) \bmod 26 = 63 \bmod 26 = 11 = L$

$D_9(E) = (4*3) \bmod 26 = 12 \text{ MOD } 26 = 12 = M$

PLAIN TEXT = ALM

Decryption

K=9 cipher text = v = 21

$D_9(L) = (L*9) \bmod 26 = 21$

لايجاد قيمة المفتاح **X** من المعادلة التالية مع العلم ان قيمة كل من المتغيرات التالية معلومة **a , n ,b** .

a X mod n = b , gcd (a, n) =1

X=[b * inv(a , n)] mod n

سنستخدم الدالة inv لايجاد قيمة X من المعادلة

$D_9(V) = (V*9) \bmod 26 = 21$

Algorithm inv(a ,n);
{
' Return x such that ax mod n = 1 where 0 < a < n '
$g_0 = n$; $g_1 = a$;
$v_0 = 0$;
$v_1 = 1$;
i=1;
while g_i <> 0 do "$g_i = u_i * n + v_i * a$;
{
$y = g_{i-1}$ div g_i ;
$g_{i+1} = g_{i-1} - y * g_i$;
$v_{i+1} = v_{i-1} - y * v_i$;
$i = i + 1$
}
x= vi-1;
if x >= 0 then inv = x else inv = x + n;
}

example

9X mod 26 = 21

V(1)= 1 v(0) =0 g(0)= n =26 g(1)=a = 9 b = 21
step1 I = 1
y=g(i-1)div g(i)= g(0) div g(1)= 26 div 9 = 2
g(i+1) = g(i-1) –y*g(i)=g(0) – y * g(1) = 26 -2*9 =26-18 = 8 = g(2)
v(i+1) = v(i-1)-y*v(i) = v(0) – y * v(1)= 0 – 2 * 1 = -2 = v(2)
step2 I =2
y=g(i-1)div g(i)= g(1) div g(2)= 9 div 8 = 1
g(i+1) = g(i-1) –y*g(i)= g(1) - y*g(2) = 9 -1 * 8 = 1 = g(3)
v(i+1) = v(i-1)-y*v(i) = v(1)- y * v(2) = 1 - 1*- 2= 3 = v(3)
step 3 I = 3

y=g(i-1)div g(i)= g(2) div g(3)= 9 div = 1
g(i+1) = g(i-1) –y*g(i)= g(2) - y*g(3) = 8 -1*8 = 0 = g(4)
v(i+1) = v(i-1)-y*v(i) = v(2)- y * v(3) = -2 – 1*3 = -5 = v(4)

g(4)= 0 inv= v(i-1) = 3
inverse = (21*3) mod 26 = 63 mod 26 = 11 = L
11 * 9 mod 26 = 21

Affine cipher

Multiplication w3 and Addition can be combined to give an affine cipher

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

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

EXAMPLE (1) : Encrypt plain text = ALMO using Affine cipher with KEY1 =4 KEY2=7 ?

Message = "ALMO"
KEY1 = 7
KEY2 = 4
$E_{k1,k2}(M) = ((M * k1)+k2) \bmod 26$

$E_{7,4}(A) = ((0 * 7) + 4) \bmod 26 = 4 = E$
$E_{7,4}(L) = ((11 * 7) + 4) \bmod 26 = 81 \bmod 26 = 3 = D$
$E_{7,4}(M) = ((12 * 7) + 4) \bmod 26 = 88 \bmod 26 = 10 = K$
$E_{7,4}(O) = ((14 * 7) + 4) \bmod 26 = 102 \bmod 26 = 24 = Y$

Cipher text = EDKY

Example (2):- Plaintext= "OMAR "and K_1 =3 and K_2 =2
Using the same table of alphabet
C(O) = (14*3+2) mod 26 = 44 mod 26 = 18 → S
C(M) = (12*3+2) mod 26 = 38 mod 26 = 12 → M
C(A) = (0*3+2) mod 26 = 2 → C
C(R) = (17*3+2) mod 26 = 53 mod 26 = 1→ B

∴ C= "SMCB"

Example (3):- encrypt and decrypt Plaintext= " HELLO " and key (7, 2)
This means K_1 =7 and K_2 =2
C(H) = (07*7+2) mod 26 = 51 mod 26 = 25 → Z
C(E) = (04*7+2) mod 26 = 30 mod 26 = 4 → E
C(L) = (11*7+2) mod 26 = 79 mod 26 = 1 → B
C(L) = B
C(O) = (14*7+2) mod 26 = 100 mod 26 == 22 → W

∴ C= ZEBBW

Now for deciphering "ZEBBW" with key pair (7, 2):-
k^{-1} (7)=15
P=(C-K_2)*K_1^{-1} mod 26

P(Z) = ((25-2)* 15) mod 26 =(23*25) mod 26 = 345 mod 26 =7 → H
P(E) = ((4-2)* 15) mod 26 =2*15 mod 26 =30 mod 26 = 4 → E
P(B) = ((1-2)* 15) mod 26 =-1*15 =-15mod 26 =(26-15)=11 → L
P(B) = L
P(W) = ((22-2)*15) mod 26 =14 → O

∴ P= "HELLO"

Key Word mixed

We need keyword like MATHEMATIC, and follow the steps:

1- Remove the repeated letters from keyword
2- Put the first letter of the modified keyword under the key letter flowed by the remaining letters of the keyword.
3- Complete the cipher text alphabet by the remaining letters without repetitions .

Ex
Plaintext = "ALMAMONUNIVERSITY"
KEY ="MATHMATIC"
1- KEY =MATHIC"

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

2-Cipher text =**BRSBSVUAUOTJYZOMI**

3- Decryption

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

Plaine text = ALMAMONUNIVERSITY

=Transposed keyword mixed

We need keyword like MATHEMATICS, and follow the steps:

1- **Remove the repeated letters from keyword (MATHEICS)**
2- **Put it in matrix and rest of alphabet following last key letter**

The letters from the keyword form the headings of the columns, and the remaining letters of the alphabet

fill in order in the rows below. Mixing is achieved by transcribing columns.

Example: If the keyword is REGINA, then write

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

so that transcribing columns left-to-right gives the substitution

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

plaintext = ALMAMONCOLLEGE
JKFCIIIIN7cipher text= RJKRKMLGMJJNBN
7J9-88+6

Autokey Cipher

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

Encryption: $C_i = (P_i + k_i) \bmod 26$ Decryption: $P_i = (C_i - k_i) \bmod 26$

Example

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.

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

	M	**T**	**M**	**T**	**C**	**M**	**S**	**A**	**L**	**H**	**R**	**D**	**Y**
	12	**19**	**12**	**19**	**2**	**12**	**18**	**0**	**11**	**7**	**17**	**3**	**24**
K	**12**	**0**	**19**	**19**	**0**	**2**	**10**	**8**	**18**	**19**	**14**	**3**	**0**
	0	**19**	**-7**	**0**	**2**	**10**	**8**	**-8**	**-7**	**-12**	**3**	**0**	**24**
mod	**0**	**19**	**19**	**0**	**2**	**10**	**8**	**18**	**19**	**14**	**3**	**0**	**24**
	A	**T**	**T**	**A**	**C**	**K**	**I**	**S**	**T**	**O**	**D**	**A**	**Y**

Vigenere Cipher

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

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**

	H	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**
c	**7**	**7**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**2**	**6**
key	**15**	**0**	**18**	**2**	**0**	**11**	**15**	**0**	**18**	**2**	**0**	**11**	**15**	**0**
c-k	**-8**	**7**	**4**	**8**	**18**	**11**	**8**	**18**	**-7**	**4**	**13**	**8**	**-13**	**6**
mod	**18**	**7**	**4**	**8**	**18**	**11**	**8**	**18**	**19**	**4**	**13**	**8**	**13**	**6**
	S	**H**	**E**	**I**	**S**	**L**	**I**	**S**	**T**	**E**	**N**	**I**	**N**	**G**

Homophonic substitution

Replace each letter with a variety of substitutes ,the number of potential sublimities being proportional of the frequency of the letter

A	**10**	**13**	**34**	**48**	**54**	**67**	**79**	**93**			
B	**49**	**82**									
C	**14**	**42**	**63**								
D	**02**	**04**	**46**	**80**							
E	**15**	**17**	**25**	**47**	**56**	**58**	**65**	**75**	**83**	**88**	**99**
F	**91**	**31**									
G	**07**	**26**									
H	**24**	**40**	**51**	**57**	**66**	**68**					
I	**33**	**71**	**73**	**83**	**88**	**94**					
J	**16**										
K	**05**										
L	**27**	**38**	**52**	**85**							
M	**23**	**28**									
N	**19**	**59**	**60**	**67**	**72**	**92**					
O	**01**	**05**	**07**	**54**	**72**	**90**	**44**				
P	**39**	**96**									
Q	**95**										
R	**30**	**36**	**41**	**53**	**78**	**81**					
S	**12**	**20**	**37**	**77**	**87**	**97**					
T	**18**	**21**	**31**	**44**	**50**	**70**	**76**	**86**	**98**		
U	**09**	**62**	**64**								
V	**35**										
W	**60**	**90**									
X	**29**										
Y	**22**	**53**									
Z	**03**										

Ex :
Plain text : A L M A M O N C O L L E G E
Cipher text = 54 27 28 48 23 01 19 14 05 38 52 17 26 25

Beale cipher

We assign a set of numbers to each letter in the plain text alphabet by using a specific text, each letter in the plain text will be replaced by number that represent the location of some ward in the text that start with this letter.

1 2 3 4 5 6 7 8 9 10 11 12 13
Substitution in which each element in the plain text (bit, letter, group of
14 15 16 16 17 18 19 20 21 22 23 24
bits or letters) is mapped into another element, and transposition, in which
25 26 27 28 29 30 31 32 33 34
each element in the plain text are rearranged. The fundamental
35 36 37 38 39 40 41 42 44 45
requirement is no information be lost (that is, all operations are
46 47 48 49 50 51 53 53 54 55

Ex
Plain text = A L M A M O N C O L L E G E
Cipher text = 19 11 17 21 47 44 62 63 58 16 40 20 12 20

Decryption
Cipher text = 19 11 17 21 47 44 62 63 58 16 40 12 20
Plain text = A L M A M O N C O L L G E

Hill Cipher (encryption)

$C = (K \times P) \bmod 26$

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

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

EXAMPLE:

P = "PAY MORE MONEY"

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

$$\begin{matrix} C1 \\ C2 \\ C3 \end{matrix} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} P \\ A \\ Y \end{pmatrix} \text{ MOD 26}$$

$$\begin{matrix} C1 \\ C2 \\ C3 \end{matrix} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} \text{ MOD 26}$$

C1= 17*15 + 17*0 + 5*24 = 11 = L
C2= 21*15 + 18*0 + 21*24 = 13 = N
C3= 2*15 + 2*0 + 19*24 = 18 = S

<u>DECRYPTION</u>

C= LNSHDLEWMTRW

$$K^{-1}K = KK^{-1} = I$$

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

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

$K\ K^{-1} \bmod 26 = I$

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} 448 & 442 & 442 \\ 858 & 492 & 780 \\ 494 & 52 & 365 \end{pmatrix} \mod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

EXAMPLE

Example :Decryption

C= LNSHDLEWMTRW

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} L \\ N \\ S \end{pmatrix}$$

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix}$$

P_1= (4*11 + 9*13 + 15*18) MOD 26 = 15 = P

P_2= (15*11 + 17*13 + 6*18) MOD 26 = 0 = A

P_3= (24*11 + 0*13 + 17*18) MOD 26 = 24 = Y

EXAMPLE

P = EG $\quad K = \begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix} \quad K^{-1} = \begin{pmatrix} 15 & 20 \\ 17 & 9 \end{pmatrix}$

C = K × P MOD 26

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} 4 \\ 6 \end{pmatrix} \text{ MOD } 26 = \begin{pmatrix} 24 \\ 16 \end{pmatrix}$$

C_1 = Y ; C_2 = Q

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} 15 & 20 \\ 17 & 9 \end{pmatrix} \begin{pmatrix} 24 \\ 16 \end{pmatrix} \text{ MOD } 26 = \begin{pmatrix} 4 \\ 6 \end{pmatrix}$$

$P_1 = E$; $P_2 = G$

One time pad

Simple substitution and transposition ciphers individually do not provide a very high level of security. However, by combining these transformations it is possible to obtain strong cipher.

A product cipher combines two or more transformations in a manner intending that the resulting cipher is more secure than the individual components.

As will be seen some of the most practical and effective symmetric-key systems are product ciphers. One example of a product cipher is a composition of t ≥ 2 transformations E_{k1} E_{k2} ….E_{kt} Where each F_i, $1 \leq i \leq t$, is either a substitution or a transposition. For the introduction purpose, let the composition of a substitution and a transposition be called a round.

Example:

Let M = C = k be the set of all binary strings of length six. The number of elements in M is $2^6 = 64$. Let m = (m1m2……m6) and define:

$E^{(1)}_k (m) = m \oplus k$, where $k \in K$;

$E^{(2)}_k (m) = (m4m5m6m1m2m3)$.

Here, $\oplus$ is the exclusive-OR (XOR) operation defined as follows:

$0 \oplus 0 = 0$ $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$, $E^{(1)}_k$ is a substitution cipher (not involving the key). The product $E^{(1)}_k$ $E^{(2)}_k$ is a round. While here the transposition cipher is very simple and is not determined by the key, this need not be the case.

EXAMPLE
Encryption

M = A=65=1000001
K = B=66=1000010

$E^{(1)}_k(m) = m \oplus k = 0000011$

m1 = 0 m2 = 0 m3 = 01 m4 = 0 m5 = 0 m6 =1 m7 = 1

$E^{(2)}_k(m) = (m4m5m6m1m2m3m7) = (0010001)$

Decryption

D2(m) = m1m2m3m4m5m6m7 = 00000011

C= 0000011

K= 1000010

$D^{(1)}_k(c) = c \oplus k = 1000001 = 65 = A$

The Vernam Cipher:

It is a type of one time pad devised by Gilbert Vernam for AT & T. The Vernam Cipher is immune to most cryptanalytic attacks. A motivating factor for the Vernam Cipher was its simplicity and ease of implementation.

Example:

We will perform a Vernam encryption in decimal notation. Assume that the alphabetic letters are combined by sum mode 26 with a stream of random two-digit numbers.

If the message is: VERNAM CIPHER
The letters would first be converted to their numeric equivalents, as shown here:

Plain text= V E R N A M C I P H E R
Wight = 21 4 17 13 0 12 2 8 15 7 4 17

Next we need some random numbers to combine with the letter codes. Suppose the following series of random two-digit numbers is generated.

Key = 76 48 16 82 44 03 58 11 60 50 48 88

The encoded form of the message is the sum mod 26 of each coded letter with the corresponding random number.

plainText	V	E	R	N	A	M	C	I	P	H	E	R
Weight	21	4	17	13	0	12	2	8	15	7	4	17

Random.No.	76	48	16	82	44	03	58	11	60	50	48	88
SUM	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
Cipher text.	T	A	H	R	S	P	I	T	X	M	A	b

Q Decrypted the following cipher text "ZDAKOL" by using Vernam and the key = 33 25 24 19 10 18 the plane text.
a- school b- Secret c- Sunday d- spaces

	Z	D	A	K	O	L
	26	26	26	26	26	26
KEY	-33	-25	-24	-19	-10	-18
	-7	1	2	7	16	8
Value	+25	3	0	10	14	11
Mode 26	18	4	2	17	30	19
	18	4	2	17	4	19
	S	E	C	R	E	T

Playfair cipher

Description

The Playfair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher.

To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order (usually omitting "Q" to reduce the alphabet to fit, other versions put both "I" and "J" in the same space). The key can be written in the top rows of the table,

from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. The keyword together with the conventions for filling in the 5 by 5 table constitute the cipher key.

To encrypt a message, one would break the message into digraphs (groups of 2 letters) such that, for example, "HelloWorld" becomes "HE LL OW OR LD", and map them out on the key table. The two letters of the digraph are considered as the opposite corners of a rectangle in the key table. Note the relative position of the corners of this rectangle. Then apply the following 4 rules, in order, to each pair of letters in the plaintext:

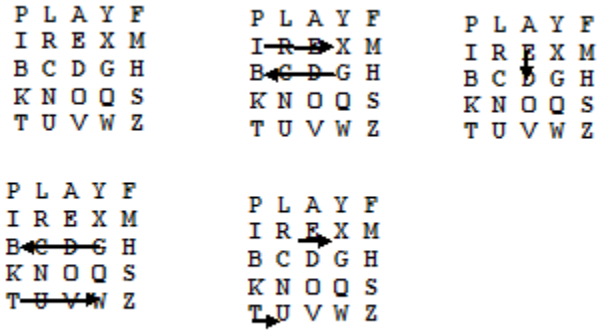
1. **If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Playfair use "Q" instead of "X", but any uncommon monograph will do.**
2. **If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).**
3. **If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).**
4. **If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.**

To decrypt, use the INVERSE (opposite) of the last 3 rules, and the 1st as-is (dropping any extra "X"s (or "Q"s) that don't make sense in the final message when finished).

Ex

Encrypting the message "Hide the gold in the tree stump":

```
      Plain text :HI DE TH EG OL DI NT HE TR EX ES TU
MP
Cippher text = BM OD ZB XD NA BE KU DM UI XM MO UV IF
```



Bifid Cipher

The first of the three rules for Playfair encipherment changes one two-letter group, or digraph, to another by exchanging column co-ordinates. This suggests using row and column co-ordinates in a more general fashion. Let's take the 5 by 5 square above, but number the rows and the columns, like this

Ex :plain = THIS IS MY SECRET MESSAGE
KEY=TXVHRLK

	1	2	3	4	5
1	T	X	V	H	R
2	L	K	M	U	P
3	N	Z	O	J	E
4	C	G	W	Y	A
5	F	B	S	D	I

T	H	I	S	I	S	M	Y	S	E	C	R	E	T	M	E	S	S	A	G	E
1	1	5	5	5	5	2	4	5	3	4	1	3	1	2	3	5	5	4	4	3
1	4	5	3	5	3	3	4	3	5	1	5	5	1	3	5	3	3	5	2	5

Porta Table

Giovanni Baptista della Porta developed the Porta Table cipher method in 1565. The table uses a keyword and the table below to encipher message.

AB	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
CD	A	B	C	D	E	F	G	H	I	J	K	L	M
	Z	N	O	P	Q	R	S	T	U	V	W	X	Y
EF	A	B	C	D	E	F	G	H	I	J	K	L	M
	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
GH	A	B	C	D	E	F	G	H	I	J	K	L	M
	X	Y	Z	N	O	P	Q	R	S	T	U	V	W
IJ	A	B	C	D	E	F	G	H	I	J	K	L	M
	W	X	Y	Z	N	O	P	Q	R	S	T	U	V
KL	A	B	C	D	E	F	G	H	I	J	K	L	M
	V	W	X	Y	Z	N	O	P	Q	R	S	T	U
MN	A	B	C	D	E	F	G	H	I	J	K	L	M
	U	V	W	X	Y	Z	N	O	P	Q	R	S	T
OP	A	B	C	D	E	F	G	H	I	J	K	L	M
	T	U	V	W	X	Y	Z	N	O	P	Q	R	S
QR	A	B	C	D	E	F	G	H	I	J	K	L	M
	S	T	U	V	W	X	Y	Z	N	O	P	Q	R
ST	A	B	C	D	E	F	G	H	I	J	K	L	M
	R	S	T	U	V	W	X	Y	Z	N	O	P	Q

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

Keyword: JACKET

Message: LOOK UNDER THE COUCH

J	A	C	K		E	T	J	A	C		K	E	T		J	A	C	K	E
L	O	O	K		U	N	D	E	R		T	H	E		C	O	U	C	H

The next step is to use the Porta table to create the enciphered message. Use the letters from the keyword (JACKET in the example above) to locate the correct line to use in the Porta table. In the example above "J" is the first keyword letter. Thus, locate "J" on the left hand side of the Porta table. Once you locate the "J", the 5th set of letters in the Porta table, you use the letter from the plain message to find the enciphered letter above or below it. In this example the value for "L" in the "J" set is "U".

Ciphertext: UBCS JJZRF LSU YBIXS

char	ascii	binary	wight
A	65	1000001	0
B	66	1000010	1
C	67	1000011	2
D	68	1000100	3
E	69	1000101	4
F	70	1000110	5
G	71	1000111	6
H	72	1001000	7
I	73	1001001	8
J	74	1001010	9
K	75	1001011	10
L	76	1001100	11
M	77	1001101	12
N	78	1001110	13
O	79	1001111	14
P	80	1010000	15
Q	81	1010001	16
R	82	1010010	17

S	83	1010011	18
T	84	1010100	19
U	85	1010101	20
V	86	1010110	21
W	87	1010111	22
X	88	1011000	23
Y	89	1011001	24
Z	90	1011010	25