Chapter Two

CLASSICAL ENCRYPTION TECHNIQUES

2.1 Cryptography Classification

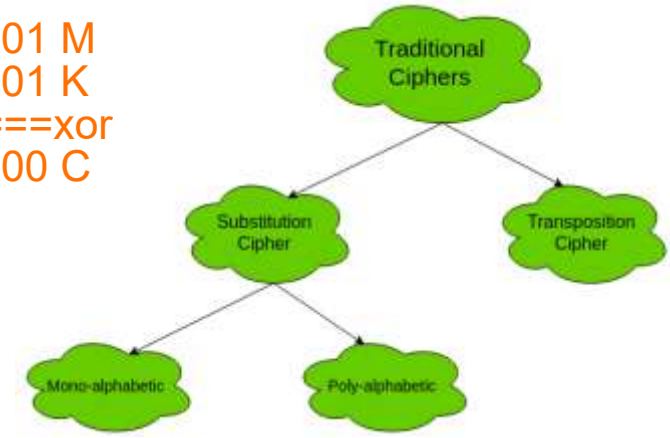
The old Encryption and Decryption techniques before the implementation of computer systems are called Classical techniques, while those invented and implemented for the computer systems are called modern techniques. However, cryptography system (whether Classical or Modern) are generally classified along three independent dimensions:

1- The **type of operations** used for transforming plaintext to cipher text. All encryption algorithm are based on general principle:

(a) Substitution,
(b) Transposition,
(c) Bit manipulation.

M=Bashar M. Nema
C=rhaasb.....
C=110110100001

1101 M
0101 K
====xor
1000 C



2- The **number of keys** used.

(a) **Symmetric:** If the same key is used by both, the sender and the receiver for encryption and decryption. It might be also called **Single key, Secret key, or Conventional encryption.**

(b) **Asymmetric:** If the sender and receiver, each were using different keys, usually two sets of keys, one for encryption and the other for decryption.

3- The **way,** in which the plantext is processed.
    - **Block cipher**: The input message is divided in blocks of elements and each block is processes at a time, producing an output block for each input block.
    - **Stream cipher**: The input elements are processed individually, producing an output as one element at a time, too.

2.2 Symmetric Cipher Model:

All traditional schemes are symmetric / single key / private-key encryption algorithms, with a single key, used for both encryption and decryption, since both sender and receiver are equivalent, either can encrypt or decrypt messages using that common key.

However, there are hundreds of traditional methods for information security which all employ (1) **Substitution** or (2) **Transposition** techniques (or both), however, they can be categorized into only two techniques, symmetric and asymmetric systems, which are well suited and implemented for computer system applications, which will be studied during the course.

The basic terminology used:

- **plaintext** - the original message
- **ciphertext** - the coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (code breaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - the field of both cryptography and cryptanalysis

A simplified model of conventional encryption/decryption system is shown in figure 2-2.

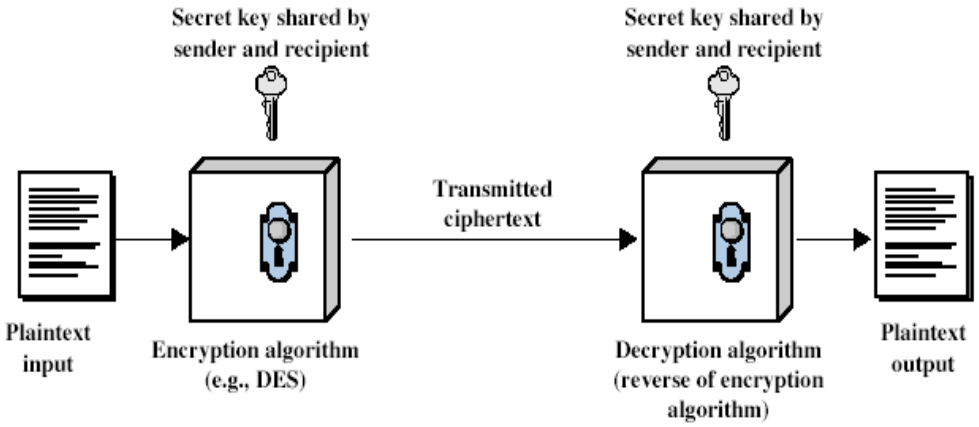


Fig. 2-2 simplified cipher model

The five ingredients of the symmetric cipher model of figure 2-1 are:

- **plaintext**
- **encryption algorithm** – performs substitutions/transformations on plaintext
- **secret key** – control exact substitutions/transformations used in encryption algorithm
- **ciphertext**
- **decryption algorithm** – inverse of encryption algorithm

Requirements:

Two requirements for secure use of symmetric encryption:

1. a strong encryption **algorithm**
2. a secret **key** known only to sender / receiver

Generally one assumes that the algorithm is known. This allows easy distribution of s/w and h/w implementations and hence assume just keeping **key secret** is sufficient to secure encrypted messages.

Having plaintext X, ciphertext Y, secret key k, encryption algorithm E_k and decryption algorithm D_k, the calculation involve

$C = E_k(Y)$ and $X = D_K(Y)$

This implies the need for secure channel to distribute key.

2.2.1 Substitution Techniques:

A substitution technique is one in which the letters of plaintext are replaced by other letters or numbers or symbols. But, if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

Few security techniques will be considered here as examples for substitution cipher.

1. Caesar Cipher:

Substitution ciphers form the first of the fundamental building blocks. The core idea is to replace one basic unit (letter/byte) with another. Whilst the early Greeks described several substitution ciphers, the first attested use in military affairs of one was by Julius Caesar, described by him in *Gallic Wars* (cf. Kahn pp83-84). Still any cipher using a simple letter shift is called **Caesar cipher**, not just those with shift 3.

Caesar cipher involves replacing each letter of the alphabet with a letter standing 3 places further down the alphabet. Therefore the alphabet transformation sets for plain and cipher are:

PLAIN: if K=3 then PLAIN= SODLQ KHUH=HERE

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

Example 1.

Encipher the message: Plaintext = "**COME HERE**" by Caesar cipher.
Solution: Ciphertext = "**FRPH KHUH**"

Example 2..

Plaintext = "**MEET ME AFTER THE TOGA PARTY**"
Ciphertext = "**PHHW PH DIWHU WKH WRJD SDUWB**"

C=(P+K)MOD 26

This mathematical description uses **modulo arithmetic** (i.e. clock arithmetic). Here, when you reach **Z** you go back to **A** and start again. Mod **26** implies that when you reach **26**, you use **0** instead (i.e. the letter after **Z**, or **25 + 1** goes to A or 0).

Mathematically, if we assign a numerical equivalent to each letter (a=1, b=2, etc.), i.e.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
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 follow: For each plaintext letter p, substitute the cipher text letter C:

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

A shift may be of any value **k**, so that the general Caesar algorithm is

$$C = E(p) = (p + k) \bmod (26)$$

Where **k** takes on a value in the range 1 to 25.

The Decryption algorithm is simply

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

2. Monoalphabetic Cipher

Arbitrary substitution of letters in the alphabet gives dramatic increase in the key space.
e.g. one possibility:

plain:	**a**	**b**	**c**	**d**	**e**	**f**	**. . .**	**x**	**y**	**z**
cipher:	**K**	**M**	**Z**	**A**	**F**	**R**	**. . .**	**D**	**S**	**E**

There is a significant improvement in the security of a message encoded by using a randomized version of the alphabet. There are **26** factorials (**26!**) ways to arrange the alphabet, with the inclusion of space, that number becomes (**27!**) ways. Therefore, **26!** Is a very large number which equals to about **4×10^{26}** possible keys.

Therefore*, this technique is quite safe using *Brute-Force, however, another line of attack is possible.

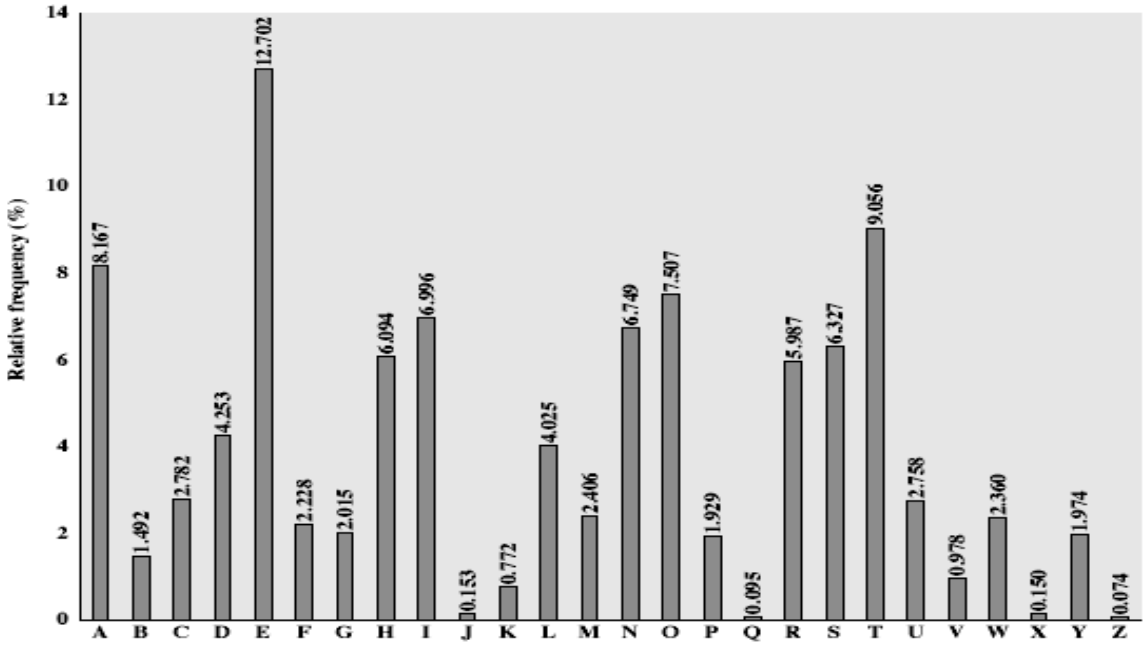


Fig. 2-3 Frequency counts for English alphabet

- **guess P & Z are e and t**
- **guess ZW is the and hence ZWP is the**
- **proceeding with trial and error finally get:**

"it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in Moscow" .

3. **Playfair Cipher:** (Invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair). This method uses multiple letter encryption cipher.

twomorrow
twomr

- a 5X5 matrix of letters based on a keyword.
- fill in letters of keyword (no duplicates)
- fill rest of matrix with other letters
- eg. using the **keyword** MONARCHY, then table 2-2 is constructed (no duplicate letters and I & J are counted as one letter).

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

Notes: Plaintext encrypted two letters at a time.

1- If a pair is a repeated letter, insert a filler like 'X',
BA LL OO N
BA LX LO ON
e.g. "balloon" encrypts as "ba lx lo on".

2- If both letters fall in the same row, replace each with letter to right (wrapping back to start from end),
e.g. “ar" encrypts as "RM".

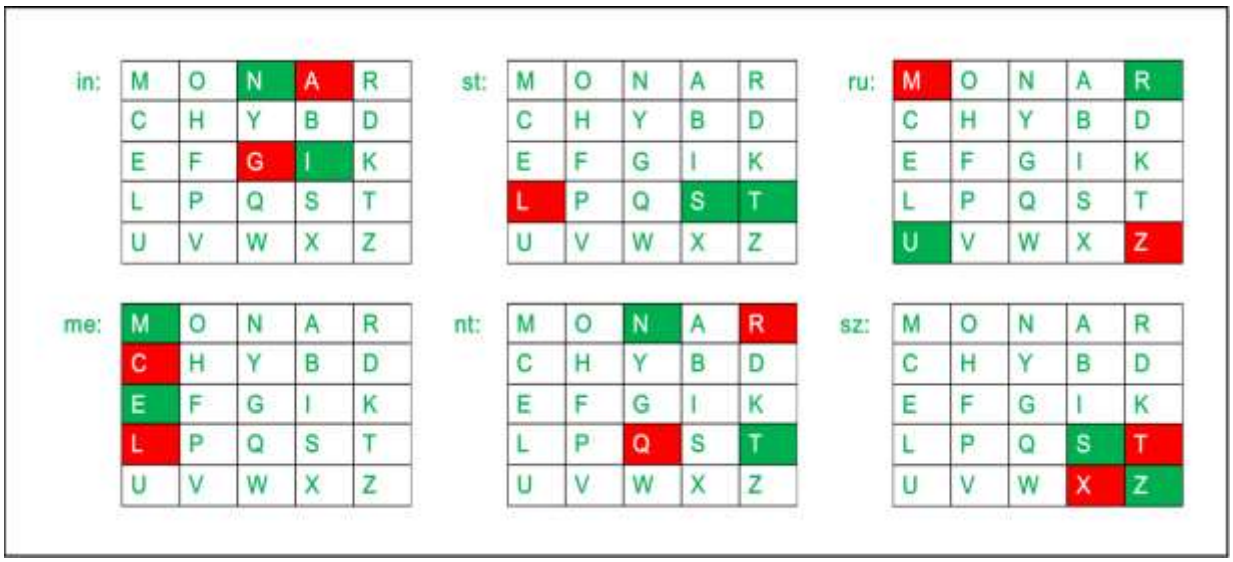
3- If both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom),
e.g. “mu" encrypts to "CM".

4- **If neither of the above rules is true**: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.
e.g. “hs" encrypts to "BP", and “ea" to "IM" or "JM" (as desired).

5- If the number of letters is odd, use a filler letter X.

6- Decryption is done in reverse direction, then remove extra X’s (or fillers).

Example1: Encrypt message “**INSTRUMENTS**”. KW=”MONARCHY”



Plain: **IN ST RU ME NT SZ**

Cipher: **GA TL MZ CL RQ TX**

DECRPTION (red)-> (green):

ga -> in tl -> st mz -> ru cl -> me rq -> nt tx -> sz

Example2: encipher the message: "**HASHIMY**".
Solution: Message is arranged in two letters: "**HA SH IM YX**", Then the Cipher will be: "**BO PB EA BW**".

Remarks: In playfair Cipher,
1- There is 26X26 = 676 diagram
2- Frequency analysis is more difficult,
i.e. it has good strength against ciphertext-only attack.

4.Hill cipher

Hill cipher is a polygraphic substitution cipher based on linear algebra.Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher. Here, the technique works as follows:

- The encryption algorithm takes **m** successive plaintext letters, substituting for **m** cipher letters according to **m** linear equations.

- Each character is assigned a numerical value:
  (a = 0, b = 1, . . . z = 25)

For **m = 3**, the system can be described as follows:

$$C1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$$
$$C2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$$
$$C3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26$$

This can be expressed in term of column vectors and matrices:-

$$\begin{pmatrix} C1 \\ C2 \\ C3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}$$

In Hill:
S/R: must agree about K.
S/R: must agree about Alphabet.
K: must be square matrix.(2X2, 3X3..)
Plain: "(ISI) (S in) (Doh)(okZ)"
: (ISI)(S i)(n D)(oHo)(kZZ)

Or $C = K P$

Where C and P are column vectors of length 3 and K is a 3X3 matrix.

Input : Plaintext: ACT

Key: GYBNQKURP ; **Key-1=** inverse matrix (IFKVIVVMI in letters)

Output : Ciphertext: POH

Encryption:

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

Decryption:

أ

K-1

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

H/W

1) i suppose that alphabet as follow:

A	B	C	D	E	F	G	H	I	J	K	L	M	NOPQRSTUVWXYZ
0	1	2	3	4	5	6	7	8	9	10	11	12	25

Input : Plaintext: GFG

Key: HILLMAGIC

Output : Ciphertext: SWK

2) COUNT CHAR IN KEY=9>3x3

$$\begin{bmatrix} 7 & 8 & 11 \\ 11 & 12 & 0 \\ 6 & 8 & 2 \end{bmatrix} \times \begin{bmatrix} 6 \\ 5 \\ 6 \end{bmatrix} = (?) \text{ MOD } 26$$

Example :
Consider the plaintext "pay more money" then use the encryption key

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

Solution:
Take m = 3, i.e. three letters at a time. If the first **three** letters of plaintext are represented by the vector (**15 0 24)** instead of **"pay", t**hen

K(15 0 24) = (375 819 486) mod 26
= (11 13 18) = LNS.

Continuing in this fashion, the ciphertext for the entire plaintext will be: "**LNSHDLEWMTRW"**

Decryption requires using the inverse of the matrix **K**. The inverse K^{-1} of the matrix K is defined by the equation $\mathbf{KK^{-1} = K^{-1}\ K = I}$, Where I is the identity Matrix.

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

This is demonstrated as follow:

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

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

We have, $\mathbf{C = E_K\ (P) = K\ P \text{ mod } 26}$ **and** $\mathbf{P = D_K\ (C) = K^{-1}\ C \text{ mod } 26}$

5. Polyalphabet Cipher:

MUSTANS I R I Y A H= PLAIN
SC I ENCES CI E N C=KEY
EW

Multi-alphabet sets are used with:

1- A set of related mono-alphabetic substitution rules is used.
2- A key determines which rule is chosen.

One famous cipher is **Vigenere** Cipher

Vigenere Cipher: Vigenere Cipher consists of 25 Caesars Cipher shifts from 0 to 25. Each is denoted by a key letter. A table is then constructed as shown in table 2-3.

Table 2-3The modern Vigenere tableau

	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

The rule of substitution:
Given a key letter X for the alphabet set and a plaintext letter **Y** for the column, i.e. in this case it is V.

Example: Encrypt the message M, where

M: **"we are discovered save yourself"**
Using Vigenere cipher with a
key: **"deceptive".**

Solution

Plaintext: **"wearediscoveredsaveyoursef"**
Key: **"deceptivedeceptivedeceptive"**
Ciphertext: ***"zicvtwqngrzgvtwavzhcqyglmgj"***

Decryption is equally simple:

1- Key letter identifies the row.
2- Ciphertext letter in the row identifies the column.
3- Plaintext letter is at the top of the column.

► A modification to prevent ciphertext letter frequency analysis attack suggest the use of key that is built from a keyword and the message itself.
i.e. for the previous example,

Key: "deceptivewearediscoveredsav"
Plaintext: "wearediscoveredsaveyoursef"
Ciphertext: "zicvtwqngkzeiigasxstslvvwla"

1) In substitution, each plaintext must be replaced with another one.
2) In Transpostion, the index of the plaintext is randomized in other order.
ex:WORD-> rwod--wrod--drow

2.2.2 Transposition Techniques

A very different kind of mapping is achieved by performing some sort of permutation on the plantext letters. This technique is referred to as a *transposition* cipher.

plaintext and KEYrepresnt depth=number

1- Rail fence Technique

ZigZaq

It is the simplest transposition cipher, in which the **plaintext** is written down as a sequence of diagonals (columns) 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 message **M** as follows:

Solution: S/R agree about depth this repsent the key and then agree about strategy (BU or TD)

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 **C** is "MEMATRHTGPRYETEFETEOAAT"

Example: Encrypt the message with Key or Depth=3 and Bottom-Up,
M: "DISCONNECT THE PLUGS NOW"

Solution:

Rewritten the message first in the form:

		S				N				T				L				N		
	I		C		N		E		T		H		P		U		S		O	
D				O				C				E				G				W

Then the ciphertext is taken as:

C: " SNTLNICNETHPUSODOCEGW" SNTLNICNETHPUSODOCEGW

Example: Encrypt the message with Key or Depth=3 and Top-Down,
M: "DISCONNECT THE PLUGS NOW"

Solution:

Rewritten the message first in the form:

2- Matrix Transposition

A more complex Scheme is to write the message in a rectangle, row by row, then 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. The blanks are filled with characters.

Example:

Encrypt the message **M** = "attack postponed until two am", using the key : 4 3 1 2 5 6 7

Solution:

Write the message **M** in a rectangle having 7 columns.

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	l	L	t
	w	o	a	m	x	y	z

TTNAAPTMTSUOAODWCOIXKNLYPETZ

The output cipher text is going to be ATTACK POST PONED UNTIL TWO AM XYZ

C: "TTNAAPTMTSUOAODNCOIXKNIPETZ"

- The transposition cipher can be made more secure by performing more than one transposition stage. The result is a more complex permutation that is not easily reconstructed.

For instant, if the output of the previous example is rewritten in a rectangle again and taking up column in the same key sequence, i.e. key: 4 3 1 2 5 6 7, then see the following:

Key:	4	3	1	2	5	6	7
Input:	t	t	n	a	a	p	t
	m	t	s	u	o	a	o
	d	w	c	o	l	x	k
	n	l	y	p	e	t	z

The output would be

C: "NSCYAUOPTTWLTMDNAOIEPAXTTOKT"

3- Code Book

Another example of the transposition cipher is the use of "**Code Book**", i.e. using a code book or table for enciphering, as shown in the following example.

Example

The code book is shown in the table:

Word	Code
BAKER	1701
FRETTING	5603
GUITARIST	4008
LOAFING	3790
.	.
.	.

For a message (plaintext):

***M**: "LOAFING BAKER"*

*The ciphertext **C**, when the code book is used will be :*

C: "3790 1701"

2.2.3 Bit-Manipulation ciphers

S/R agree about alphabet and Coding (Ascii or others

S/R must agree about KEY

Bit manipulation ciphers are well-suited for computer use because they employ operations easily performed by the system.

S/R must agree about length of coding 7-bits, 8- bits

- The ciphertext looks like unused or crashed files and thereby confusing any one who tries to gain access to the file.

- Bit manipulation ciphers covert plaintext into cipher text by altering the actual bit pattern of each character through the use of one or more of the character through the use of one or more of the following logical operations: AND, OR, NOT, XOR, 1's Complement.

► An improved method of bit-manipulation coding uses the XOR operator. The XOR operator has the following truth table

ASCII:American Standard Code for Information Interchange (A=65) (a=97)

A	B	Y
0	0	0
1	1	0
1	0	1

For example

Plaintext:	**1 1 0 1**	**1 0 0 1**
Key:	**0 1 0 1**	**0 0 1 1**

Then the Ciphertext: 1 0 0 0 1 0 1 0
