ENCRYPTION TECHNIQUES

There are two basic building blocks of all encryption techniques: substitution and transposition.

1. SUBSTITUTION TECHNIQUES:

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

Caesar cipher

The earliest known use of a substitution cipher and the simplest was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.
e.g., plain text : ALOK
Cipher text: DORN

Note that the alphabet is wrapped around, so that letter following "Z" is "A".
For each plaintext letter p, substitute the cipher text letter c such that
$C = E(p) = (p+3) \bmod 26$
A shift may be any amount, so that general Caesar algorithm is
$C = E\ (p) = (p+k) \bmod 26$

The decryption algorithm is simply
$P = D(C) = (C-k) \bmod 26$

Playfair cipher

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

The playfair algorithm is based on the use of 5x5 matrix of letters constructed using a t the keyword be „monarchy‟. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order.
The letter „i‟ and „j‟ count as one letter. Plaintext is encrypted two letters at a time
According to the following rules: Repeating plaintext letters that would fall in the same pair are separated with a Filler letter such as „x‟.

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 following the last.
Plaintext letters that fall in the same column are replaced by the letter beneath, with the top
element of the column following the last.

Otherwise, each plaintext letter is replaced by the letter that lies in its own row
And the column occupied by the other plaintext 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

Plaintext = meet me at the school house
Splitting two letters as a unit => me et me at th es ch o x ol ho us ex
Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL IU

Mono-alphabetic ciphers

In mono alphabetic cipher we not use the uniform scheme for all alphabets in a given plaintext message in thi s we decide to use random substitution. This means that in agiven plain text message, each A can replaced by any other alphabet (B through Z) , each B can also be replaced by other random alphabet (A or C through Z0, and so on. The crucial difference being there is no relation between the replacement of B and replacement of A.

Vigenere cipher

In this scheme, the set of related monoalphabetic substitution rules consisting of 26 caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter. e.g., Caesar cipher with a shift of 3 is denoted by the key value 'd‟ (since a=0, b=1, c=2 and so on). To aid in understanding the scheme, a matrix known as vigenere tableau is Constructed Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plaintext runs across the top. The process of

	PLAIN TEXT															
K		a	b	c	d	e	f	g	h	i	j	k	…	x	y	z
E	a	A	B	C	D	E	F	G	H	I	J	K	…	X	Y	Z
Y	b	B	C	D	E	F	G	H	I	J	K	L	…	Y	Z	A
	c	C	D	E	F	G	H	I	J	K	L	M	…	Z	A	B
L	d	D	E	F	G	H	I	J	K	L	M	N	…	A	B	C
E	e	E	F	G	H	I	J	K	L	M	N	O	…	B	C	D
T	f	F	G	H	I	J	K	L	M	N	O	P	…	C	D	E
T	g	G	H	I	J	K	L	M	N	O	P	Q	…	D	E	F
E R	: :	: :	: :	: :	: :	: :	: :	: :	: :	: :	: :	: :	…	: :	: :	: :
S	x	X	Y	Z	A	B	C	D	E	F	G	H	…			W
	y	Y	Z	A	B	C	D	E	F	G	H	I	…			X
	z	Z	A	B	C	D	E	F	G	H	I	J	…			Y

Encryption is simple: Given a key letter X and a plaintext letter y, the cipher text is at theintersection of the row labeled x and the column labeled y; in this case, the ciphertext is

V.

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

e.g., key = deceptivedeceptivedeceptive PT = wearediscoveredsaveyourself CT = ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plaintext letter is at the top of that column.

Polygram substitution cipher:

In the polygram substitution cipher technique rather than replacing one plain text alphabet with one cipher text alphabet at a time a block of alphabet is replaced another block.

For example: HELLO could be replaced by YUQQW, But HELL could be replaced by a totally different cipher text block TEUI,

This shows that in the polygram substitution cipher, the replacement of plain text happens block by block, rather than character by character.

Hill Cipher:

Hill cipher is a polyalphabetic cipher introduced by Lester Hill in 1929. Let us discuss the technique of hill cipher.

Plain text: Binary

Key: HILL

Choose the key in such a way that it always forms a **square matrix**. With HILL as the key, we can form a 2×2 matrix.

Now, of plain text, you have to form a column vector of length similar to the key matrix. In our case, the key matrix is 2×2 then the column vectors of plain text would be 2×1.

The general equation to find cipher text using hill cipher is as follow:

C = KP mod 26

$$(c_1\,c_2) = \begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix} \begin{pmatrix} p_1 \\ p2 \end{pmatrix} \; mod\; 26$$

For our example, our key matrix would be: $\begin{pmatrix} H & I \\ L & L \end{pmatrix}$

And our plain text matrices of 2×1 will be as follow:

$$\begin{pmatrix} B \\ I \end{pmatrix} \begin{pmatrix} N \\ A \end{pmatrix} \begin{pmatrix} R \\ Y \end{pmatrix}$$

Now, we have to convert the key matrix and plain text matrices into numeric matrices. For that number the alphabets such as A=0, B=1, C=2, …………, Z=25. So, considering the alphabet numbering:

Key matrix will be:

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

Plain text matrices would be:

$$\begin{pmatrix} 1 \\ 8 \end{pmatrix} \begin{pmatrix} 13 \\ 0 \end{pmatrix} \begin{pmatrix} 17 \\ 24 \end{pmatrix}$$

In the first calculation, we would get two cipher alphabets for plain text alphabet ‘B’ & ‘I’.

$$(c_1\,c_2) = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 1 \\ 8 \end{pmatrix} \; mod\; 26$$

$$(c_1\;c_2) = \begin{pmatrix} 71 \\ 99 \end{pmatrix} mod\; 26$$

$$(c_1\;c_2) = \begin{pmatrix} 71 \\ 99 \end{pmatrix} mod\; 26$$

$$(c_1\;c_2) = \begin{pmatrix} 19 \\ 21 \end{pmatrix}$$

$$(c_1\;c_2) = \begin{pmatrix} T \\ V \end{pmatrix}$$

So, the cipher alphabet for plain text alphabet ‘B’ & ‘I’ is ‘T’ & ‘V’. Similarly, we have to calculate ciphertext for remaining plain text. And then accumulate them to form the ciphertext.

The calculated **ciphertext** for ‘**Binary**’ using hill cipher is ‘**TVNNZJ**’.

One-Time Pad:

The one-time pad cipher suggests that the **key length** should be **as long as the plain text** to prevent the repetition of key. Along with that, the **key** should be **used** only **once** to encrypt and decrypt the single message after that the key should be discarded.

Onetime pad suggests a new key for each new message and of the same length as a new message. Now, let us see the one-time pad technique to convert plain text into ciphertext. Assume our plain text and key be:

Plain text: Binary

Key: Cipher

Now again convert the plain text and key into the numeric form. For that number the alphabets such as A=0, B=1, C=2, ………., Z=25. So, our plain text and key in numeric form would be:

Plain text: 1 8 13 0 17 24

Key: 2 8 15 7 4 17

Now, you have to add the number of the plain text alphabet, to the number of its corresponding key alphabet. That means, for this example, we will add:

B+C = 1+2 = 2

I+I = 8+8 = 16

N+P = 13+15 = 28

A+H = 0+7 = 7

R+E = 17+4 = 21

Y+R = 24+17 = 41

The resultant ciphertext numbers we get are (2, 16, 28, 7, 21, 41)

If the addition of any plain text number and the key number is >26, then subtract only that particular number from 26. We have the addition of two pair of plain text number and a key number, greater than 26, i.e. N+P=28 & Y+R=41.

Subtract them by 26.

N+P = 28 – 26 = 2

Y+R = 41 – 26 = 15

So, the final **ciphertext numbers are (2, 16, 2, 7, 21, 1)**. Now convert this number to alphabets assuming A to be numbered 0 and B to be 1…..Z to 25.

Ciphertext: Cqchvb.

In this way, we can convert plain text to cipher text using a one-time pad.

So, this is all about the substitution cipher techniques. It has a monoalphabetic cipher and polyalphabetic cipher technique. Substitution technique is also called classical substitution technique.

2. TRANSPOSITION TECHNIQUES

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

Rail fence:

is simplest of such cipher, in which the plaintext is written down as a sequence of diagonals andthen read off as a sequence of rows.

Plaintext = meet at the school house

To encipher this message with a rail fence of depth 2, we write the message as follows:m e a t e c o l o s

e t t h s h

o h u e The

encrypted

message is

MEATECOLOSE
TTHSHOHUE

Row Transposition Ciphers:

A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of columns then becomes the key of the algorithm.

e.g., plaintext = meet at the school house

Key = 4	3	1	2	5	6	7
PT = m	e	e	t	a	t	t
h	e	s	c	h	o	o
l	h	o	u	s	eCT = ESOTCUEEHMHLAHSTOETO	

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is more complex permutation that is not easily reconstructed.