Explain Caesare Cipher technique with example.

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

For example:

Plaintext : meet me after the toga party.

Ciphertext : PHHW PH DIWHU PKH 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:

Let us, assign a numerical equivalen to each letter:

a	b	c	d	e	f	g	h	i	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	t	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext: abcdefghijkl mnopqrstuvwxyz

Ciphertext: defghijklmnopqrstuvwxyzabc

Then the algorithm can expressed as follows:

For each plaintext letter, P. subtitute the ciphertext letter C

$\therefore C = E(3, P) = (P+3) \bmod 26$

A shift can be any amount. so that the general ~~plaintext~~ ~~ceasar~~ algorithm is.

$$C = E(K, P) = (P + K) \bmod 26$$

where takes on a value ~~of~~ in the range 1 to 25. The decryption algorithm follow.

~~$P = D(K, P) = ($~~

$$P = D(K, C) = (C - K) \bmod 26$$

In this case, the plaintext leaps out as occupying the third line. The three important characteristics of this ~~alphabet~~ problem enabled us to use a brute-force ~~an~~ cryptanalysis:

1. The encryption and decryption algorithm is known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily recognizable.

Encrypt the following message using Caesar cipher technique and use encryption key 134 : "meet me after the toga party".

Ans: To encryption the following message "meet me after the toga party" using Caesar cipher technique with a key 134. First we reduce the key modulo 26

$\therefore 134 \bmod 26 = 4$

Then, the effective encryption key is 4. Now, we shift the letter in the message by 4 positions in the alphabets.

Plaintext : meet me after the toga party.

Ciphertext : qiix qi ejxiv xli xske tevxc

5b Explain Mono-alphabetic cipher with an example.

– Monoalphabetic Cipher: A mono-alphabetic cipher is a type of substitution cipher where each letter in the plaintext is replaced by a fixed, different letter from the alphabet.

In mono-alphabetic Cipher, the mapping is done randomly and the difference between the letter is not uniform.

Let us consider an example, we define a substitution pattern by shifting the letters of the alphabet is randomly.

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

Now let's use this substitution to encrypt a message.

Plaintext : HELLOW

~~Ciphertext~~ : ~~OTDDHV~~ ITSSGV

Ciphertext : ITSSGV

Plaintext : UAMME

Ciphertext : GQDDT

5b Explain Playfair Cipher with Example.

= The best-known multiple-letter encryption cipher is the playfair cipher, which treats the digrams in the ~~key~~ plain text as single units and translates these units into the plaintext digrams. The playfair cipher is more secure than monoalphabetic cipher because it uses the matrix of the alphabets to perform the substitution, creating greater complexity by working with pairs of letter.

The encryption algorithm consists of two steps:

Generate the key square (5X5): The key square is 5X5 grids of the alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (each table can be hold only 25 alphabets). If the plaintext is J, then it replaced by I.

Encrypted Digraphs: The message to be encrypted divided into a pair of letters. If a pairs contains the same letters like (ll), X is inserted between them. If the message has an odd number of letters, it trailing z, is added to the final plain text.

Encryption: There are three main rules for encryption of playfair cipher each pair of letters.

1. Same Row: If both letters of the digraph appear in the same row of the matrix, each letter is replaced by the letter immediately to its rights. (wrapping around to the start of the row if needed)

Same Column: If both letters are in the same colom of the matrix, each letter is replaced by the letter immediately below it. (wrappingaround to the top if necessary)

Same Rectangle: If both the letters form the corner of the same rectangle, each letter is replaced by the one on the same row but in the other corner of the rectangle.

Example of the playfair ciphen:

Suppose, the key is Keyword. then the matrix.

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

Suppose let the plaintext message: HELLO WORLD

Then the final plaintext: HE LX LO WO RL DZ

Then the ciphertex : GY IZ SC OK CF CU

Explain the Hill cipher with an example.

Ans: Another interesting multiple letter cipher is a Hill cipher, developed by the mathematician Lester Hill in 1929. Hill cipher is a polygraphic substitution cipher based on the linear algebra. Each letter is represented by a number modulo 26. Often simple scheme is A=0, B=1 ---- Z=25 is used, but this is not an essential features of a cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertile nxn matrix, against modulo 25. To decrypted a message, each block of letter multiplied by inverse matrix for encryption.

Example: Encryption.

Suppose, A plaintext is : Hi World

and the key is : DDCF

Suppose we choose a 2x2 as our key matrix:

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

let, encrypt the plaintext : Hi World
the final plaintext : Hi Wo rl dx

2. Convert plaintext to the number:

Hi using mapping A=0, B=1 --- Z=25

- H → 7
- I → 8
- W → 22
- O → 14

r → 17
l → 11
d → 3
x → 23

So the plaintext vector is:

$$P_1 = \begin{bmatrix} 7 \\ 8 \end{bmatrix} \quad P_2 = \begin{bmatrix} 22 \\ 14 \end{bmatrix} \quad P_3 = \begin{bmatrix} 17 \\ 11 \end{bmatrix} \quad P_4 = \begin{bmatrix} 3 \\ 23 \end{bmatrix}$$

We will now encrypt each pair of letter using the formula:

$$C = K \cdot P \bmod 26$$

∴ First pair:

$$C_1 = K \cdot P_1 \bmod 26$$

$$= \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 21+24 \\ 14+40 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 45 \\ 54 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 19 \\ 2 \end{bmatrix}$$

So the ciphertext for HI is tC

2nd Pair:

$$C_2 = KP_2 \bmod 26$$

$$= \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 22 \\ 14 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 108 \\ 114 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 4 \\ 10 \end{bmatrix}$$

So the ciphertext for wo is ek

3rd Pair:

$$C_3 = KP_3 \bmod 26 = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 17 \\ 11 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 84 \\ 89 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 6 \\ 11 \end{bmatrix}$$

So, the ciphertext for nl is gL

4th Pair:

$$C_4 = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 3 \\ 23 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 78 \\ 121 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0 \\ 17 \end{bmatrix}$$

So, the ciphertext for dn is ar

Then the final ciphentext for Hi world is tc ekglar

Decryption:

Given the ciphentext "TC EKGLAR and the key matrik.

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$ and

then the inverse matrix of K is

$$K^{-1} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

The ciphetctex vecton is

$$C_1 = \begin{bmatrix} 19 \\ 2 \end{bmatrix} \quad C_2 = \begin{bmatrix} 4 \\ 10 \end{bmatrix} \quad C_3 = \begin{bmatrix} 6 \\ 11 \end{bmatrix} \quad C_4 = \begin{bmatrix} 0 \\ 17 \end{bmatrix}$$

We will now decrypt each letter pair using formular

$$P = K^{-1} C \bmod 26.$$

$$\therefore P_1 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 19 \\ 2 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 319 \\ 398 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 8 \end{bmatrix} = hi$$

$$P_2 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 4 \\ 10 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 230 \\ 170 \end{bmatrix} \bmod 26 = \begin{bmatrix} 22 \\ 14 \end{bmatrix} = WO$$

$$P_3 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 6 \\ 11 \end{bmatrix} \bmod 26$$

$= \begin{bmatrix} 17 \\ 11 \end{bmatrix} = rL$

$P_4 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 0 \\ 17 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 3 \\ 23 \end{bmatrix}$

$= dx$

Exa

* Explain Vigenere Cipher with an example.

Ans: The Vigenere Cipher is a type of polyalphabetic substitution cipher, was developed by th the 16th century by the France cryptographer Blaise de Vigenere We can express the vigenere cipher in the following manner:

Assume a sequence of the plaintext letter $P = P_0, P_1, P_2 -- P_{n-1}$, a key consisting the sequence of the letter $K = k_0, k_1 --- k_{m-1}$, typically $m < n$. The sequence of the ciphertext letter $C = C_0, C_1, C_2 --- C_{n-1}$ is calculated as follows.

$$C = C_0, C_1, C_2 -- C_{n-1} = E(K, P) = E(k_0, k_1, k_2 -- k_{n-1}. P_0, P_1 --- P_{m-1}) \bmod 26$$

$$= (P_0 + K_0) \bmod 26, (P_1 + K_1) \bmod 26 --- (P_{m-1} + K_{m-1}) \bmod 26, (P_m + K_0) \bmod 26, (P_{m+1} + K_1) \bmod 26 ---- (P_{2m-1} + K_{m-1}) \bmod 26 .....$$

Thus, the first letter of the key is added to the first letter of the plaintext. the second letter are added and so on through the first m letter of the plaintext. For this next m letter of the plaintext, the key letters

are repeated. This process is continued until all the sequence of plaintext is encrypted. A general equation of the encryption process is -

$$C_i = (P_i + K_i \bmod m) \bmod 26$$

Then, the generalization of the decryption equation is

$$P_i = (C_i - K_i \bmod m) \bmod 26$$

Example: If the key is 'deceptive' and the plain-text message is "we are discovered save yourself" is encrypted as:

Key : deceptivedeceptiveeceptive

Plaintext: wearediscoveredsaveyourself

Key	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4
plain text	22	4	0	17	4	3	8	18	2	14	21	4	17	4	3	18	0	21	4	24	14	20	17	18	4	11	5
cipher	25	8	2	21	19	22	16	13	6	17	25	6	21	19	22	0	21	25	7	2	16	24	6	11	12	6	9

Ciphertext: zicvtwqngrzgvtwavzhcqyglmgj

Explain the Vernam Ciphur with an example.

= The Vernam Cipher is a method of encrypting alphabetic text. It is one of the substitution techniques and converting the plaintext into ciphertext.

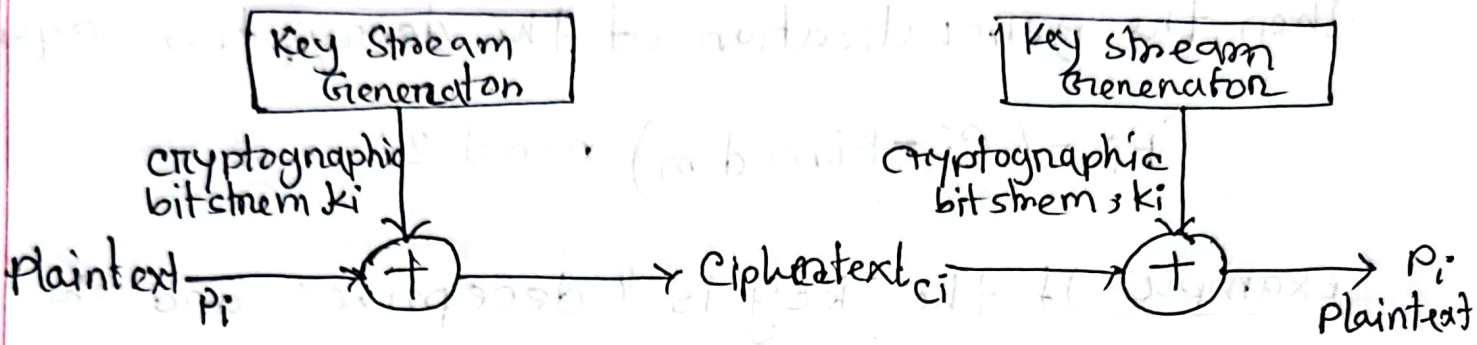

Fig: Veranam Cipher -

This system works on binary data (bits) rather than the letters. This system can be express succinctly as follows:

$$C_i = P_i \oplus K_i$$

where, ~~P_i = ith the di number of di~~

P_i = ith binary digit of plaintext.

C_i = ith the binary digit of Ciphertext.

K_i = ith the binary digit of key.

$\oplus$ = Ex-clusive OR operation.

Thus, the ehip> ciphertext is generated by performming the bitwise XOR of the plaintext and the key. Because of the properties of XOR, decryption simply involves the same bitwise operations.

$$P_i = C_i \oplus K_i$$

Example: Encryption:

Suppose, the key is FIRST and the plaintext message is UAMME

Plaintext position (P) :	20	0	12	12	4
Key position (K) :	5	8	17	18	19
(P+K)	25	8	29	30	23
Ciphertext position(C)	25	8	3	4	23

Ciphertext : ZIDEX

Decryption:

Ciphuntextpasition(C) :	25	8	3	4	23
Key position (K)	5	8	17	18	19
(C-K)	20	0	14	-14	4
plaintext position (P)	20	0	12	12	4

plaintext : UAMME