Q.4. Encrypt the following message using Caesar Cipher technique and use encryption key 134: "meet me after the toga party"

Have given,

plaintext ± meet me after the toga party.

and key, k = 134

Let us, assign a numerical equivalent 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

We know, The general Caesar algorithm is

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

$$= (p + 134) \bmod 26$$

∴ For each plaintext letter p, substitute the ciphertext letter C as:

plain : meet me after the toga party

Here, p = each plaintext letter, C = ciphertext letter

For example, p = a = 0, k = 134

$$\therefore C = (0 + 134) \bmod 26$$

$$= 4 = e$$

For each plaintext letter, p substitute the ciphertext letter c as

plain: meet me after the toga party

cipher: qiix qi ejxiv xli xsketevxc

Q.5 Explain Caesar cipher technique with example.

Explanation of Caesar cipher technique: The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

let us assign a numerical equivalent 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

We know, The general Caesar algorithm is

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

Here, C = ciphertext letter, p = plaintext letter, k = key

For example, $p = 0$, $k = 3$

$$\therefore C = (0 + 3) \bmod 26$$
$$= 3$$

Similarly, 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
cipher:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

plain:	s	t	u	v	w	x	y	z
cipher:	V	W	X	Y	Z	A	B	C

Consider a plaintext as Hello Rahatul

For each plaintext letter p, substitute the ciphertext letter C. as

plain : Hello Rahatul

cipher : KHOOR UDKDWXO

Finally, if it is known that a given ciphertext

Now, the decryption algorith is simply

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

Decryption as follow

After decryption,

Cipher : KHOOR VDKDWXO

plain : Hello Rahatul

Finally, if it is know that a given ciphertext is a caesar cipher, then a brute-force cryptanalysis is easily performed.

Q.6 Explain mono-alphabetic cipher with example?

Explanation: The 'cipher' line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than 4×10^{26} possible keys. This ~~is 10 orders of magnitude greater than the key space for DES~~. This would seem to eliminate brute-force techniques for cryptanalysis. Such an approach is ~~reffer~~ referred to as a monoalphabetic substitution cipher, because a single cipher alphabet is used per message.

If the cryptanalyst knows the nature of the plaintext, then the analyst can exploit the regularities of the language.

To see how such a cryptanalysis might proceed, Consider an example. The ciphertext to be solved is ~~AETEH~~ mo
As a first step, the relative frequency of the letter can be determined and compared to a standard frequency distribution for English.

In this case, the relative frequencies of the letters in the ciphertext. (in percentages) are as follows

O = 40 M = 20 N = 20 C = 20	otherwise = 0

Comparing this breakdown with standard frequency distribution for English, it seems likely that cipher letters M is the equivalents of plain letters a. And the letters M, N and C are probably correspond to plain letters from the set {r, h, t}.

So far, we have,

A E T E H MONOC
r a h t r a h a t

Hence, the complete plain text as follows

rahat

Finally, we can say that, monoalphabetic ciphers are easy to break the reflect frequency data of the original alphabet.

Q.7 Encrypt the following message using Playfair cipher technique and use encryption key "MONARCHY":

"I am Improving"

Have given, the keyword is MONARCHY

and plaintext: I am Improving

We know, The playfair algorithm is based on the use of a 5×5 matrix of letters constructed using a keyword as following, as...

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

Here,

Plaintext is encrypted two letters at a time,

I a m i m p r o v i n g

S B A E O L M N X F Y Q

plaintext: I am Improving

cipher: SBAEOLMNXFYQ

Q.8 Explain Playfair Cipher with example?

The best-known multiple-letter encryption cipher is the Playfair, which treats diagrams in the plaintext as single units and translates these units into ciphertext diagram.

The playfair algorithm is based on the use of a 5×5 matrix of letters constructed using a keyword. Here in an example,

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

In this case, the keyword is MONARCHY.

Here,

Plaintext is encrypted two letters at a time, according to the following rules.

1. Repeating plaintext letters that are in the same pair separated with a filler letter. Such as 'balloon' would be treated as ba lx lo on
2. Two plain text letters that ~~are~~ fall in the same row of the matrix are each replaced by the letter to the right. For example, ar is encrypted as RM

3. 'Two plaintext letters that fall in the same column are each replaced by the letter beneath. 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.

For Complete example,

Plaintext : I am improving

Cipher : SB AE OL MN

plaintext : Ia mi mp ro vi ng

Cipher : SB AE OL MN XF YQ

Q.9 Explain Hill cipher technique in details.

Hill cipher is multiletter cipher. This encryption algorithm takes m successive plaintext letters and substitutes for them m ciphertext letters. The substitution is determined by m linear equations in which each character is assigned a numerical value (a=0, b=1, ..., z=25). For m=2, the system can be described as

$$C_1 = (k_{11} P_1 + k_{12} P_2) \bmod 26$$

$$C_2 = (k_{21} P_1 + k_{22} P_2) \bmod 26$$

This can be expressed ~~in terms of~~ as.

$$(C_1 \; C_2) = (P_1 \; P_2) \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} \bmod$$

or, $C = PK \bmod 26$

where, C and P are row vectors, representing the ciphertext and plaintext.

and K = the encryption key.

For example, plaintext: 'Hill' is encrypted using 2x2 Hill cipher,

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

and $K = \begin{pmatrix} 3 & 2 \\ 8 & 5 \end{pmatrix}$ key, $K = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$\therefore C = \left[\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 8 & 5 \end{pmatrix} \right] \bmod 26$$

$$= \begin{pmatrix} 85 & 54 \\ 121 & 77 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 7 & 2 \\ 17 & 25 \end{pmatrix}$$

ciphertext : HCRZ

Also, The decryption algorithm expressed as

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

Here, $$K^{-1} = \frac{Adj(K)}{|K|}$$

Q.10. Explain polyalphabetic cipher in details.

The best known, and one of the simplest, polyalphabetic ciphers is the Vigenere cipher. In this scheme, the set of related monoalphabetic substitution rules consists of the 26 caesar ciphers with shifts of 0 through 25.

We can express the Vigenere cipher in the following manner. Assume a sequence of plaintext letters $P = P_0, P_1 \cdots P_{n-1}$ and key $K = k_0, k_1 \cdots, k_{m-1}$ where $m < n$. The sequence of ciphertext letters $C = C_0, C_1 \cdots C_{n-1}$ is calculated as follows,

$$C = C_0, C_1 \cdots C_{n-1} = E(k, P)$$

$$= (P_0 + k_0) \bmod 26, (P_1 + k_1) \bmod 26 \cdots$$

A general equation of the encryption process is

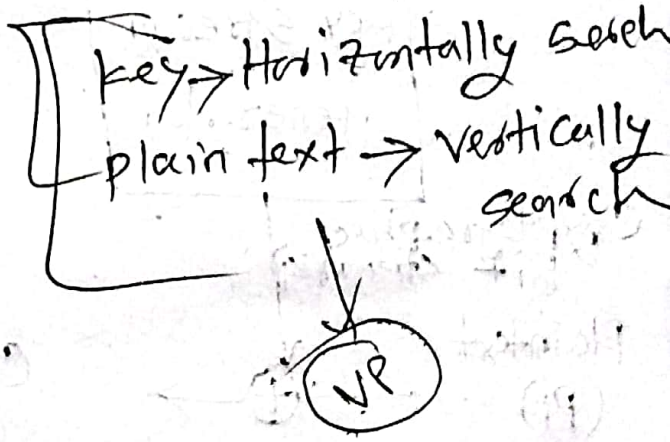
$$C_i = (P_i + k_{i \bmod m}) \bmod 26$$

Similarly, decryption is a generalization of is

$$P_i = (C_i - k_{i \bmod m}) \bmod 26$$

For example, if the keyword is abc, and the message is "Bad" then encrypted as

	A	B	C	D	E	
A	A	B	C	D	E	...
B	B	C	D	E	F	...
C	C	D	E	F	G	...
D	D	E	F	G	H	...
E						



we have following result

key	0	1	2
plaintext	1	0	3
Ciphertext	1	1	5

Finally, key : abc
plaintext : Bad
Ciphertext : BBF

Similarly, The decryption process is; ~~$P_i = (C_i - K_i \bmod m)$~~

$$P_i = (C_i - K_{i \bmod m}) \bmod 26$$

Therefore; Polyalphabetic proposed is referred to as an autokey system, in which a keyword is concatenated with the plaintext itself to provide a running key

Q. 11 Explain Vernam Cipher in details.

Vernam Cipher works on binary data (bits) rather than letters. The System can be expressed succinctly as follows

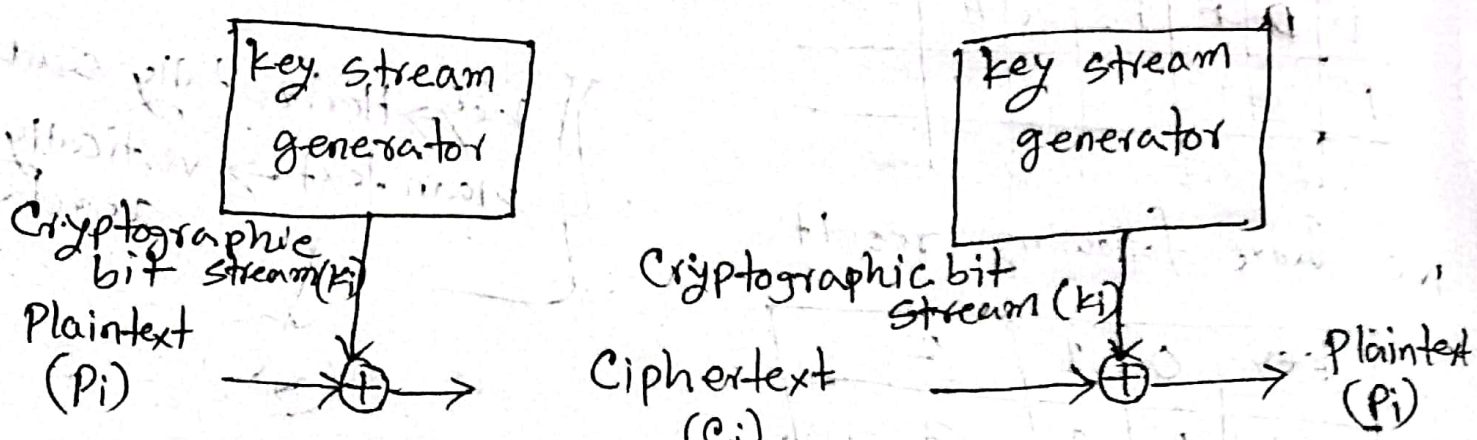


Figure. 2.7 : Vernam Cipher.

From the following Figure 2.7, we can write,

$$C_i = P_i \oplus K_i$$

where, P_i = ith binary digit of plaintext

K_i = ith " " " key

C_i = ith " " " Ciphertext

$\oplus$ = exclusive-OR (X-OR) operation.

Thus, the ciphertext is generated by performing the bitwise XOR of the plaintext and the key.

→ Vernam proposed the use of a running loop of tape that eventually repeated the key.

Q.12 Explain One-Time pad Technique with example.

When each new message requires a new key of the same length as the new message; such a scheme, known as a one-time pad, is unbreakable.

It produces random output that bears no statistical relationship to the plaintext. Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.

The one-time pad is of limited utility and is useful primarily for low-bandwidth channels requiring very high security.

The one-time pad is the only cryptosystem that exhibits what is referred to as perfect secrecy.

For example,

With a rail fence of depth 2, we write the following,

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 is

MEMATRHTGPRYETEFETEOAAT

This sort of thing would be ~~trival~~ trivial to cryptanalyze

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~~ Column) for example

Plaintext = attack Post poned until two am

key = 4 3 1 2 5 6 7

(কলাম বসবার sequence অনুযায়ী value দিতে হবে)

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	i	l	t
	w	o	a	m	x	y	z

Ciphertext: TTNAAPTMTSUOAODWCOIX

KNLY PETZ