Assignment 2 19UCS122

Q1. Explain Symmetric Cipher Model

->

Ingredients of Symmetric Encryption

1. Plaintext

original intelligible message

2. Encryption algorithm

performs substitutions, transformations

input: plaintext, key. output: ciphertext

3. Secret Key

different keys -> different outputs,

substitutions and transformations

4. Ciphertext

unintelligible scrambled message

depend on plaintext and key

5. Decryption algorithm

encryption algorithm run in reverse

input: ciphertext, key. output: plaintext

19UCS122

Q2. Explain Conventional Cryptosystems Model

->

Requirements

• two requirements for secure use of symmetric encryption:

- a strong encryption algorithm
- a secret key known only to sender / receiver

$Y = E_K(X)$

$X = D_K(Y)$

• assume encryption algorithm is known

• implies a secure channel to distribute key

• can characterize by:

- type of encryption operations used

• substitution / transposition / product

• Substitution: elements in plaintext mapped into another element

• Transposition: elements in plaintext are rearranged.

• Product: multiple stages of substitutions, transpositions

19UCS122

- number of keys used
• single-key or private / two-key or public
- way in which plaintext is processed
• block/stream
• Block: One block of elements at a time, producing an output block
• Stream: processes input elements continuously, producing output one element at a time.

19UCS122

Q-3 Explain following substitution cipher with e.g.

a) ceaser

The earliest known and the simplest, use of a substitution cipher was by Julius Ceaser The Caeser cipher involves replacing each letter of the alphabet with the letter standing 5 places further down the alphaber. for e.g.

Plain: meet me after the toga party.

Cipher: PHHW PH DIWHU WKH 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 possibility as follows:

plain	a	b	c	d	e	f	g	h	I	J	K	L	M	N	o	P	Q								
cipher	D	E	f	G	H	I	J	K	L	M	N	o	P	Q	R	S	T								
plain	R	S	T	U	V	W	X	Y	Z																
cipher	U	V	W	X	Y	Z	A	B	C																

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									
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16									
R	S	T	U	V	W	X	Y	Z																	
17	18	19	20	21	22	23	24	25																	

Then algorithm can be expressed as follows. for each plaintext letter P, Substitute the ciphertext letter C^2.

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

b) Mono-alphabetic

With only 25 possible keys, the Ceaser cipher is far from secure. A dramatic increase in the key space can be acheived by allowing an arbitary substitution. Before Proceding first we define Permutation.
A Permutation of a finite set of elements S is an ordered sequence of all the elements of S, with each element appearing exactly once. for e.g - if $S = \{a, b, c\}$ there are six permutations of S.
abc, acb, bac, bca, cab, cba.

In general, there are n! permutations of set of n elements, because the first element can be choosen in one of n ways, the second in n-1 ways, the third in n-2 ways & so on.
Recall the assignment for the Ceaser Cipher

ain:	a	b	c	d	e	f	g	h	I	J	K	L	M	N
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	O	P	Q	R	S	T	U	V	W	X	Y	Z		
	R	S	T	U	V	W	X	Y	Z	A	B	C		

If, instead, 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 and would seem to eliminate brute force techniques

for cryptanalysis. Such an approach is reffered to as a monoalphabetic Substitution cipher, because a single cipher alphabet is used per message.

c) Playfair Cipher.

The best known multiple letter encryption cipher is the playfair, which treats dig in the plaintext as single units & translates these units to ciphertext dig.

The playfair algorithm is based on the use of a 5x5 matrix of letters constructed using a keyword. Here is an e.g.-

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, the keyword is monarchy. The matrix is constructed by filling in the letters of the keyword from left to right and from top to bottom, and then filling in the remainder of matrix with the remaining letters in alphabetic order. The letters I & J count as one letter. Plaintext is encrypted two letters at a time, according to the following Rules-

1. Repeating Plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.

2. Two 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 circularly following the last, for e.g- ar is encrypted as RM
3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. for e.g- mu is encrypted as CM.

d) Hill Cipher -

Another intresting multiletter cipher is the Hill Cipher, developed by the mathematicial Lester Hill in 1929.

Before describing the hill cipher, let us briefly reviewe some terminology from linear algebra. In this discussion, we are concerned with matrix arithmetic modulo 26. for the reader who needs a refresher on matrix multiplication & inversion.

We define the inverse M^{-1} of a square matrix M by the eqn $M(M^{-1}) = M^{-1}M = I$. Where I is identity matrix that is all zero except for once along the main diagonal from upper left to lower right. The inverse of a matrix does not always exist but when it does, it satisfies the preceiding eqn. e.g:

$$A = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix} \quad A^{-1} \bmod 26 = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$$

19UCS122

$$AA^{-1} = \begin{pmatrix} 53 & 130 \\ 156 & 79 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

To explain how the inverse of a matrix is computed, we begin with the concept of determinant. for any square matrix (m×m) the determinant equals the sum all the Products that can be formed by taking one element from each row.

Q-5 Encrypt the following text using -Ceaser Cipher
"GCUA VQ DTGCM"

→ Considering 5 places further:

plaintext	a	b	c	d	e	f	g	h	I	J	K	L	M
Cipher	D	E	f	G	H	I	J	K	L	M	N	O	P

Plain	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
cipher	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

GCUA VQ DTGCM

∴ Result: JFXD YT GWJFP

19UCS122

Q.4 find encrypted msg using ceaser cipher & monoalphabetic cipher
⇒ "It was disclosed yesterday"

→ Ceaser Cipher →
It was disclosed yesterday

3 places further
⇒ Lw zdv GlvfoRvHG BHvWHUGDB

encrypted msg is : lw zdv glvforvhg - Bhvwhugdb.

Monoalphabetic Ceaser Cipher.

In monoalphabetic cipher, you can substitute any alphabet to the given letter. But it should not be repeated in the same word.

Randomly mapping can be done so we can not find uniform difference for all the plaintext & ciphertext scheme.

for - It was disclosed yesterday
ab mNT QatdfhtIQ KJTbJLQN

This can be replaced as:-

I → a	a → N	C → d	E → J
T → b	S → T	L → f	Y → K
W → M	d - Q	O → H	R → L

Result - It was disclosed yesterday
ab mnt qatdfhtJq KjtbjLqNK

Q.6 Explain Autokey System.

The Periodic nature of the keyword can be eliminated by using a non repeating keyword that is as long as the message itself. Vigenère Proposed what is refered to as an autokey System, in which a keyword is concatinated with the plaintext itself to provide a running key. for eg -

key : deceptivewearediscoveredsav
Plaintext : Wearediscoveredsaveyourself
ciphertext : ZICVTWQNGKZEIGASXSTSLVVWL

Even this scheme is vulnerable to Cryptanalysis. Because the key and the plaintext share the same frequency distribution of letters, a statistical technique can be applied ex - e enciphered by e, by fig 2.5, can be expected to occur with a frequency of $(0.127)^2 \approx 0.016$ whereas t enciphered by t would occur only about half as often. These regularities can be exploited to achieve successful Cryptanalysis.

VERNAM CIPHER:

The ultimate defense against such a cryptanalysis is to choose a keyword that is as long as the plaintext & has no statistical relatn to it.

19UCS122

Q.7 Explain One time Pad Substitution Technique

→ In one time Pad, each new message requires a new key of same length as the new message. Such 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 whatsever about the plain text, there is simply no way to break the code.

① There is Practicle Problem of making lo quantities of random keys. Any heavily used System might require millions o random characters on a regular basis. Supplying Truely truely random value characters in this volume is a Signi cant task.

② Even more daunting is the Problem of key distribution & protection. For every message to be sent, a key of equal length is needed by both sender & receiver. Thus, a mammo key dist^n problem exists.

③ It uses a random key of the same length message (as long as the mess

④ Here key is not repeated.

⑤ Sender is generating new key for every new msg while Sending msg to receiver so it is called as one time Pad.

PlainText H O W A R E Y O U

→ 7 14 22 0 17 4 24 14 20

Key N C B T Z Q A R Y

13 2 1 19 25 16 0 17 23

Total -	20	16	23	19	42	20	24	31	43
26 if > 25	20	16	23	19	16	20	24	5	17
	↓	↓	↓	↓	↓	↓	↓	↓	↓

Ciphertext U Q X T Q U Y F R

Q.8 Encrypt the message "meet me at usual place" using hill cipher with key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

→ A B C D ---- W X Y Z

0 1 2 3 22 23 24 25

The Plain Text

M E E T M E AT USUAL PLACE

12 4 4 19 12 4 0 19 20 18 20 0 11 15 11 0 2

Key is given = $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$

19UCS122

Key is of 2×2 matrix.

∴ we divide ~~letters~~ text in group of 2 letter

∴ Plain Text be:

ME ET ME AT US UA LP LA CE

∴ By formula,

$$(C_1, C_2) = (P_1\ P_2) \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix} \bmod 26$$

① for ME

$$(C_1, C_2) = (12\ \ 4) \begin{matrix} 12 \\ 4 \end{matrix} \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 128 \\ 64 \end{pmatrix} \bmod 26$$

$$= (128\ \ 64) \bmod 26$$

$$= \left(\frac{128}{26}\ \ \frac{64}{26}\right)$$

$$= (20, 10)$$

② for ET

$$(C_3, C_4) = (4, 19) \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 8 \\ 23 \end{pmatrix}$$

③ for ME again same as that of ①

④ for AT,

$$(C7, C8) = (0, 19) \begin{pmatrix} 9 & 5 \\ 4 & 7 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 24 \\ 5 \end{pmatrix}$$

⑤ for US

$$(C9, C10) = (20, 18) \begin{pmatrix} 9 & 5 \\ 4 & 7 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 4 \\ 8 \end{pmatrix}$$

⑥ for UA

$$(C11, C12) = (20\ 0) \begin{pmatrix} 9 & 5 \\ 4 & 7 \end{pmatrix} \bmod 26$$

$$= (22\ 18)$$

⑦ for LP

$$(C13, C14) = (11\ 15) \begin{pmatrix} 9 & 5 \\ 4 & 7 \end{pmatrix} \bmod 26$$

$$= (25\ 23)$$

⑧ for LA

$$(C15, C16) = (11\ 0) \begin{pmatrix} 9 & 5 \\ 4 & 7 \end{pmatrix} \bmod 26$$

$= (22\ \ 8)$

(f) for CE.

$$(C_{17}, C_{18}) = (2, 4) \begin{pmatrix} 9 & 5 \\ 4 & 7 \end{pmatrix} \bmod 26$$

$$= (14, 10)$$

∴ The ciphertext is

M	E	E	T		M	E	A	T	O	S	U	A	L	P	L	A	C	E
20	10	8	23		20	10	24	3	14	18	22	18	25	23	22	8	14	10
U	K	I	X		U	K	Y	D	E	I	W	S	Z	X	W	I	O	K

Cipher text :

MEET ME AT USUAL PLACE

UKIX UK YD EIWSZ XWIOK

19UCS122

Q.9 Encrypt the plain text "Send more money" using one time pad version of Vigenere Cipher with the key stream 9, 0, 1, 7, 23, 15, 21, 14, 11, 11, 2, 8, 9

A	B	C	- - -	X	Y	Z
0	1	2		23	24	25

Key is - 9 0 1 7 23 15 21 14 11 11 2
J A B H X P V O L L C

Key is 8 9
I J

plain →	S	E	N	D	M	O	R	E	M	O	N	E	Y
	18	4	13	3	12	14	17	4	12	14	13	4	24
key-	J	A	B	H	X	P	V	O	L	L	C	I	J
	9	0	1	7	23	15	21	14	11	11	2	8	9
Total-	27	4	14	10	35	29	38	18	23	25	15	12	33

If total is greater than 26, then Substract 26 from it
∴ Result of Total is

→ 1 4 14 10 9 3 12 18 23 25 15 12 7
B E O K J D M S X Z P M H

∴ Ciphertex of "Send more money" is
BEOK JDMS XZPMH

Q.10 Explain transposition Technique and encrypt the following text using railfense technique with key size = 4 / PT = " there are attacking from north" also decryption.

→ ① Transposition Techniques -

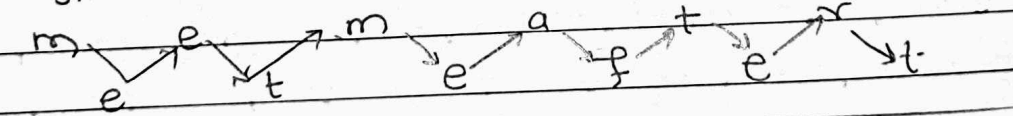
All the techniques examined so far involve the substitution of a ciphertext symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read of as sequence of rows.

e.x -

as a key = 2 Plaintex = meet me after the toga party.

Encryption can be done as:



∴ Ciphertext - firstly consider uppler line & then lower line.

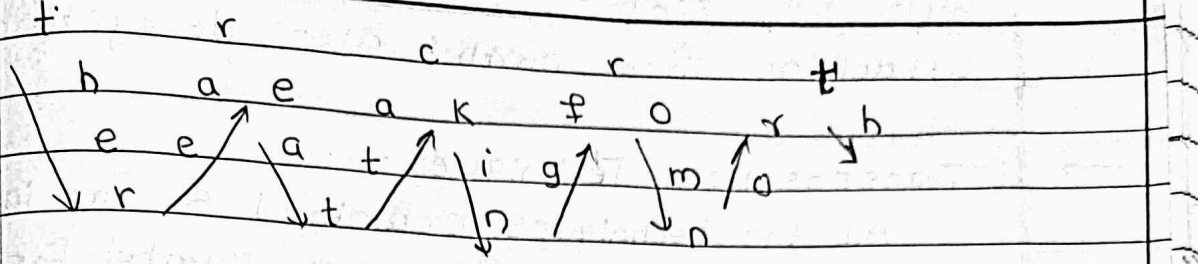
∴ ____

m e m a t r h t g p r y e t e f e t

e o a a t.

19UCS122

② for Key = 4 &
Plain Text = " there are attacking from north"



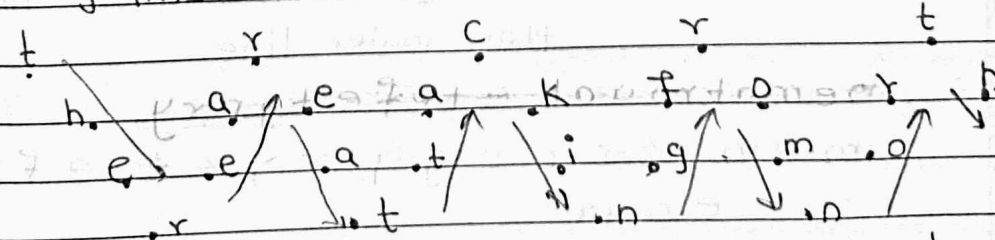
∴ Ciphertext which is encrypted from plaintext is,

trcrthaeaKforheeatigmortnn

∴ Now,
trcrthaeaKforheeatigmortnn
this is given encrypted ciphertext
we have to decrypt it to plaintext

∴ for key = 4 make 4 rail & mark the characters count = 26

& then write the ciphertext letters line by line.



& consider plain text as top to bottom as shown arrow

∴ We get plaintext by decryption is:
"There are attacking from North"

Q.11 Perform encryption operation using Playfair cipher technique.

Plaintext = "It was disclosed yesterday"

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

← key

If both are in same column as Sd then take letter at the bottom of S first i.e - Y & then consider bottom of d as K
∴ Cd = YK

Plaintext Pair :- It Wa Sd is cl os ed ye st er da yx

∴ Ciphertext →
As both letters are in different row & different column then
IT → I → Consider first row for 1st letter
T → then consider T column for 2nd letter.

∴ Ciphertex is :-
Plaintext - It Wa Sd is cl os ed ye st er da yx
Cipher :- NR EM YK KR OC CT CA VC TP LQ FB ZY

∴ The ciphertext of "It was disclosed yesterday" is :- "NR EMYK KROCCTCA VCTPLQFBZY"