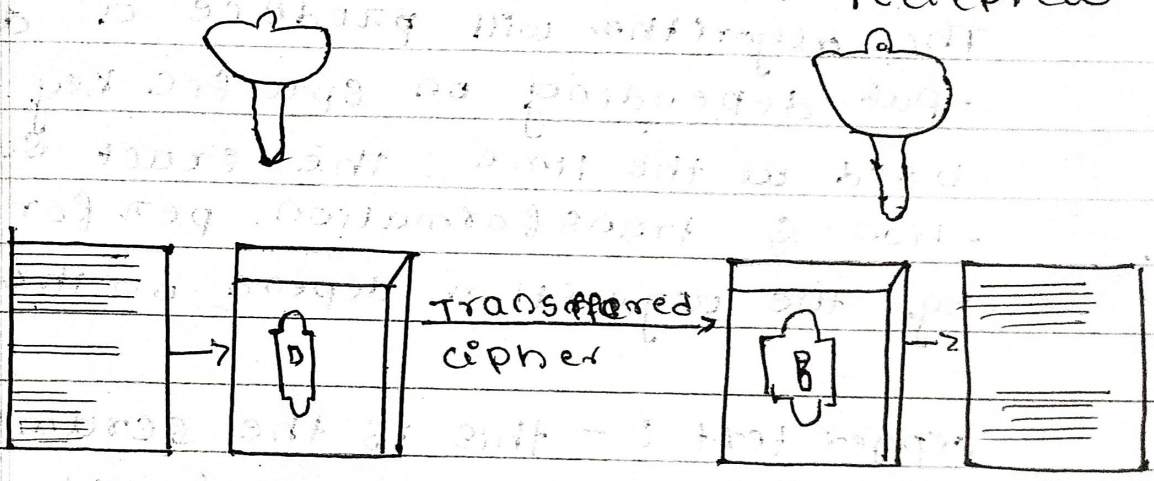
Assignment - I

1) Define cryptography & explain symmetric cipher model ?

→ It is a technique for providing a communication using the confidentiality, integrity and security.

Symmetric cipher model :-



plaintext input — encryption algorithm (eg. DES) — decryption algorithm (reverse of encryption algorithm) — plaintext output.

A Symmetric encryption scheme have five ingredients they are :

plain text : This is the original intelligible message or data that is fed into the algorithm as input.

Encryption algorithm :- The encryption algorithm performs various substitution and transformation on the plaintext.

Secrete key :- The secrete key is also input to the encryption algorithm the key is a value independent of the plain text & of the algorithm. The algorithm will produce a different output depending on specific key being used at the time. The exact substitution & transformation performed by the algorithm depends on the key

Cipher text :- this is the scrambled message produced as output. It depends on the plain text and the secret key for given message, two different key will produce two different cipher texts

The cipher text is an apparently random stream of data and as it stands is unintelligible

Decryption algorithm : this is essential The encryption algorithm run in

reverse it take the cipher text and the secrete key and produces original plaintext

Q 2) Explain Hill cipher and apply it to encrypt plain text = paymore money

with $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{bmatrix}$

pay (15, 0, 24)

$$(C_1, C_2, C_3) = (15, 0, 24) \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15\times17 + 0\times21 + 24\times2 \\ 15\times17 + 0\times18 + 24\times2 \\ 15\times5 + 0\times21 + 24\times9 \end{bmatrix} \bmod 26$$

$$= [303, 303, 531] \bmod 26$$

$$= [17, 17, 11]$$

$$= R, R, L$$

mor (12, 14, 17)

$$= (12, 14, 17) \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 12\times17 + 14\times21 + 17\times2 \\ 12\times17 + 14\times18 + 17\times2 \\ 12\times5 + 14\times21 + 17\times19 \end{bmatrix} \bmod 26$$

$$[532, 490, 677] \bmod 26$$

$$[12, 22, 1]$$

m w b

emo = [4, 12, 14]

$$= [4, 12, 14] \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 4\times17 + 12\times21 + 14\times2 \\ 4\times17 + 12\times18 + 14\times21 \\ 4\times5 + 12\times21 + 14\times19 \end{bmatrix} \bmod 26$$

$$= [348, 312, 583] \bmod 26$$

$$= [10, 0, 18]$$

= K, A, S

key = (13, 4, 24)

$$= (13, 4, 24) \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 13\times17 + 4\times21 + 24\times2 \\ 13\times17 + 4\times18 + 24\times21 \\ 13\times2 + 4\times2 + 24\times19 \end{bmatrix} \bmod 26$$

$$= [353, 341, 605] \bmod 26$$

$$= (15, 3, 7)$$

$$= (p, D, h)$$

Ciphertext = RRL MWB KAS PDH

Another interesting multiletter cipher is Hill cipher, developed by mathematician Lester Hill in 1929. The encryption algorithm takes in successive plain text letter and substituter for them in cipher text letters. The substitution is determined by an liner equations in which each character is assigned a numeric value (a=0, b=1 - - - - z=25). For m=3 the system can be described as followed $c = kp \bmod 26$ where c = ciphertext k = key and p = plain text

Q4) Explain Feistel encryption and decryption in detail.

PAGE NO.
DATE / /

—> Feistal cipher is the execution of two or more simple cipher in sequence in such a way that the final or product is cryptographically stronger than any of the component ciphers.

Feistel encryption

* The inputs to the encryption algorithm are a plaintext block of length 2w bits and a key K. The plaintext block is divided into two halves Lo and Ro
* The two halves of the data pass through n rounds of the data processing and then combine to produce The ciphertext block
* Each round i has inputs Li-1 and Ri-1 derived from the previous round as well as subkey Ki derived from overall K.
* The subkey Ki are different from K and from each other

Feistel decryption :-

* The process of decryption with a festel cipher is essentially the same as encryption process.

* The rule is as follows: use the ci
- phertext as input to the algorithm
but use the subkeys K_i in reversed
order
* That is use K_{16} in first round,
K_{16}-I in the second round, so on
until K_1 is used in last round
* The output of first round of the
decryption process is equal to a
32-bit swap of the input to the
16th round of encryption process.
* first consider encryption process

$$LE_{16} = RE_{15}$$

$$RE_{16} = LE_{15} \times F(RE_{15}, K_{16})$$

On decryption side. $LD_1 = RD_0 = LE_{16} = RE_{15}$

$$RD_1 = LD_0 \times F(RE_{15}, K_{16})$$
$$= RE_{16} \times F(RE_{15}, K_{16})$$
$$= [LE_{15} \times F(RE_{15}, K_{16})] \times F(RE_{15}, K_{16})$$

=the XOR has the following pro-
-perties : $[A \times B] \times C = A \times [B \times C]$ $D \times D = 0$

$$E \times 0 = E$$

Then $LD_1 = RE_{15}$ and $RD_1 = LE_{15}$ The o/p of first round of decryption processor is $LE_{15} || RE_{15}$ which is

PAGE NO.

DATE / /

32-bit swap of i/p to 16^{th} round of encryption

For i^{th} iteration of encryption algorithm $LE_i = RE_i - 1$

$RE_i = LE_{i-1} \times F(RE_{i-1}, K_i)$

rearranging terms, $RE_{i-1} = LE_i$

$LE_{i-1} = RE_i \times F(RE_{i-1}, K_{i2}$

$RE_i \times F(LE_i, K_i)$

③ explain playfair cipher and its rules for the following example :-
Ex:- keyword : "MONARCHY" plain text :
a) ATTACK b) CRYPTOGRAPHY

—> * A playfair algorithm is based on the use of 5x5 matrix of letters constnectid using a keywork.

Rules : Diagram

* Same row : if both letters are in same row replace each letter to its right
* Same column : if both letters are is same column replace each with below letter
* Rectangle : if letters form a rectangle replace each letter on same row but at the corner

a] keyword : MONARCHY
plain text : ATTACK

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

Diagram : AT TA CK
RS SR DE

PAGE NO.
DATE / /

b] CRYPTOGRAPHY

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

diagram : CR XP TO QR AP HX
DM HQ PR KN OS YB

7) List and explain the block cipher design principles.

-> There are three critical aspects of block cipher design:

i) The number of rounds : The greater the number of rounds the more difficult it is to perform encryptanalysis even for a relatively weak F.

* The creation should be that the number of rounds is chosen so that know cryptanalytic efforts require greater effort than a simple brute-force key search attack

* If DES had 15 or fewer rounds, differential cryptalysis would require use effort than brute - force key

Search.

ii) Design of function F :-

* The function F provides the element -s of confusion in a feistel cipher ,want it to be difficult to "unscra -mble" The substitution performed by F
* one obvious criterion is that F be nonlinear. The more nonlinear F, the more difficult any type of ~~end~~ cryptanalysis will be.
* one of the most intense areas of research in the field of symmetric block ciphers is that of S-box design. would like any change to the input vector to an S-box to result in random -looking chang -es to the output. the relationsh -ip should be non-linear and difficult to approximate with linear functions

iii) Key scheduling :- A final area of block cipher design and one that has received less attention than S-block ~~drag~~ design is the key schedule algorithm with any

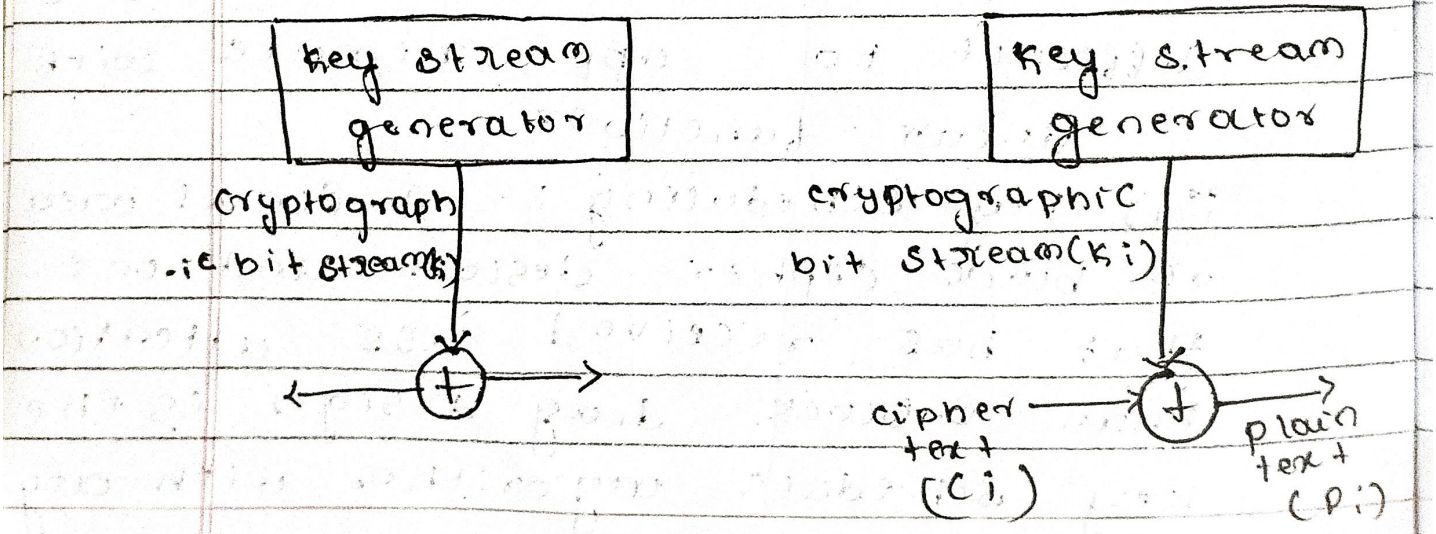
feistel block cipher. The key schedule is used to generate a subkey for each round

* would like to select subkeys to maxi-mize the difficulty of reducing individual subkeys and difficulty of working back to main key. The key schedule should guarntee key/cipher text strick Available criterio-n and bit independence criterion

8) Explain vernam cipher and OTP

* The ultimate defense against sucha cryptonalysis is to choose a keyword that is as long as the plaintext and has no statistical relationship to it

* such a system was introduced by an AT & T engineer named Gilbert vernam in 1918.



The system can be expressed succinctly as follows.

$$C_i = P_i \oplus K_i$$

where P_i = i^{th} binary digit of plaintext

K_i = i^{th} binary digit of key.

c_i = i^{th} binary digit of ciphertext

$\oplus$ = exclusive-or generated by performing the bitwise XOR of the plaintext and key. Because of the properties of XOR, decryption simply involves the same bitwise operation:

$$P_i = C_i \oplus K_i$$

One-time pad:

* The key is to be used to encrypt and decrypt a single message, and then is discarded.
* 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.
* The one-time pad offers complete security but in practical has two fundamental difficulties.

i) There is the practical problem of making large quanti-ties.

of random keys.

ii) Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver.

10. List the difference b/w conventional and public key encryption.

conventional	public key
- Needed to work: 1. The same algorithm with the same key is used for encryption and decryption	Needed to work: 1. One algorithm is used for encryption & related algorithm for decryption with a pair of keys, one for encryption and one for decryption
* The sender and receiver must share algorithm & key	* The sender and receiver must each have one of the matched pair of keys.
- Needed for security * the key must be kept secret	need for security * one of the two keys must be kept secret.

* it must be impo -ssible or at lea -st impractal to decipher a message if the key is kept secre -te.	* it must be impos -sible or at least impractical to deci -pher a message if one of the key is kept se -cret
* knowledge of the algorithm plus samples of ciphe -r text must be insufficient to determine the key	* knowledge of the algorithm plus one of the keys plus samples of cipher text must be insu -fficient to dete -rmine the other key