CS549: CNS HW 1

I) Review Questions ⇒ 1.3, 3.4, 3.12, 4.4, 4.6

Q1.3

Sol: A passive attack attempts to learn or make use of information from the system but does not affect system resources. The goal of opponent is to obtain information is being transmitted.

↳ Types of passive attacks:

a) The release of message content

In this, we would like to prevent an opponent from learning the contents of these transmissions (telephonic conversation, email message, transferred file)

b) Traffic analysis

The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. The information might be useful in guessing the nature of the communication that was taking place.

Active attacks

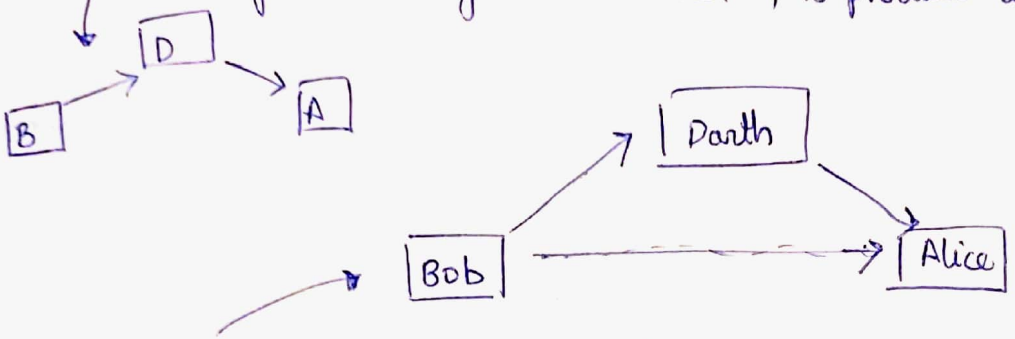
A active attack attempts to alter system resources or affect their operations. It involves some modification of the data stream or the creation of a false stream

↳ Types of active attacks:

a) Masquerade: It take place when one entity pretends to be a different entity. It involves one of the other form of active attacks.

② Modification of messages

It means that some portion of a legitimate message is altered, or that messages are delayed or recorded, to produce an unauthorized effect.



③ Replay : It involves passive capture of a message and its subsequent the transmission to produce an authorized effect.

④ ~~Masquerade~~ Repudiation

The sender or receiver can deny later that he/she has send or receive a message

⑤ Denial of service

It prevents or inhibits the normal use or management of communication facilities.

Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

Q 3.4

Both Block and Stream cipher are the methods of encryptions and belong to the family of symmetric key ciphers

	Block Cipher	Stream Cipher
1. [Definition]	Block Cipher is the type of encryption where the conversion of plain text performed by taking its block at a time	the conversation of plain text performed by taking one byte of the plain text at a time.
2. [Conversion of Bits]	Takes one block at a time so more bits get converted as compared to in Stream Cipher. (specifically 64 b)	At most 8 bits could get converted at a time
3. [Principle]	Uses both Confusion and diffusion principle for the conversion required for encryption	Only uses confusion principle for the conversion
4. [Algorithm]	for encryption, uses Electronic Code book and Cipher Block Chaining algorithm	It uses CFB (Cipher Feedback) and OFB (o/p feedback) algorithm.
5. [Decryption]	As combination of more bits get encrypted so the reverse encryption or decryption is comparatively complex	It uses XOR for the encryption which can be easily reversed to the plain text.
6. [Implementation]	The main implementation of Block Cipher is Fiestel Cipher	Main implementation of Stream Cipher is Vernam Cipher.

Q 3.12

One time pad is an encryption technique that cannot be ~~hacked~~ cracked, but requires the use of a single-use pre-shared key that is no smaller than the message being sent.

In this technique, a plaintext is paired with a random secret key (one-time pad)

The one time pad offers complete security but, in practice, has two fundamentals difficulties:

1. There is practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task
2. 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.

Q4.4

Substitution is a method of encrypting in which units of plaintext are replaced with the ciphertext, in a defined manner, with the help of a key. The units may be single letters, pairs of letters, mixture of the above. The receiver deciphers the text by performing the inverse substitution process to extract the original message.

Permutation : A sequence of plain text elements is replaced by a permutation of that sequence. That is, no elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed.

eg simple substitution

flee at once

↓↓↓↓ ↓↓ ↓↓↓↓

SIAA ZQ LKBA

permutation

m o n o a

1 2 3 4 5

↳ o a m n o

4 5 1 3 2

Q4.6 The exact realization of a Feistal network depends on the choice of the following parameters and design features.

- **Block Size**: Larger block size mean greater security but reduced encryption decryption speed. A block size of 64 bits is a reasonable tradeoff and has been nearly universal in block cipher design. However, the new AES uses a 128 bit block size.
- **Key Size** : Larger key size means greater security but may decrease encryption/decryption speed. Key sizes of 64 bits or less are now widely considered to be inadequate and 128 bits has become a common size.

- Number of Rounds : The essence of the Feistal Cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. A typical size is 16 Rounds.

- Subkey generation algorithm : Greater complexity in this algorithm should lead to greater difficulty of cryptoanalysis.

- Round function : Again, greater complexity generally means greater resistance to cryptoanalysis.

There are two other considerations in the design of a Feistal cipher

- Fast & software encryption / decryption : In many cases, encryption is embedded in application or utility functions in such a way as to preclude a hardware implementation. Accordingly, the speed of execution of the algorithm becomes a concern.

- Ease of analysis : Although we should like to make our algorithm as difficult as possible to cryptanalyze, there is great benefit in making the algorithm easy to analyze.

Numerical Problems !! ⇒ 3.1, 3.3, 4.2, 4.6

P3.1

Given Affine Caeser Cipher $C = E([a,b], p) = (ap+b) \bmod 26$

(a) No, there are no limitations on the value of b.

It satisfies the values 0 to 25.

because if the change in 'b' value can shift the ciphertext to the left or to the right of the plain text then it can be coded to the plain text similarly by the generalized form.

Therefore, it doesn't matter as long as mapping is one-to-one.

(b) Values of 'a' which are not allowed :

2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24.

Consider $a=4, b=1$ and $p=0$ or 13

at $p=0$

$C = E([4,1], 0) = (4 \times 0 + 1) \bmod 26 = 1 \bmod 26 = 1$

at $p=13$

$C = E([4,1], 13) = (4 \times 13 + 1) \bmod 26 = 53 \bmod 26 = 1$] same.

It is not one to one

(c) The values allowed by 'a' are 1,3,5,7,9,11,15,17,19,21,23,25

Values above 25 can be mapped to one of these values when mod 26 is performed.

⇒ for p, q $(0 \le p \le q \in 26)$ $c_1 = c_2$

$E(a,p) = E(a,q)$ (values not allowed)

$(ap+b) \bmod 26 = (aq+b) \bmod 26$

$c_1 - c_2 = (ap+b - aq-b) \bmod 26$

$c_1 - c_2 = a(p-q) \bmod 26$

if $a(p-q)$ is divisible by 26 then $c_1 = c_2$

Therefore $a(p-q)$ and 26 should be relative prime (no factor other than 1), because there is no way to reduce the fraction $a/26$ and $(p-q)$ is less than 26

3.3 According to standard frequency distribution for English E & T are most frequent and second most frequent letter respectively.

index of E = 4
index of T = 19 (from 0)

Given most frequent cipher text C & Z
index of C = 2
index of Z = 25

$$2 = (4a+b) \bmod 26 \longrightarrow (1)$$
$$25 = (19a+b) \bmod 26 \longrightarrow (2)$$

Solving both equations.

$$25-2 = [(19a+b)-(4a+b)] \bmod 26$$
$$23 = (15a) \bmod 26$$
$$(15a-23) \bmod 26 = 0$$

by trial & Error $a = 1, 2, 3, 4, 5 \ldots$

$$a=5, \Rightarrow (15*5-23) \bmod 26$$
$$\Rightarrow (75-23) \bmod 26 = 52 \bmod 26 = 0$$

Now putting $a=5$ in eq (I)

$$2 = (4*5+b) \bmod 26$$
$$(20-2+b) \bmod 26 = 0$$
$$(b+18) \bmod 26 = 0$$
$$b = 8$$

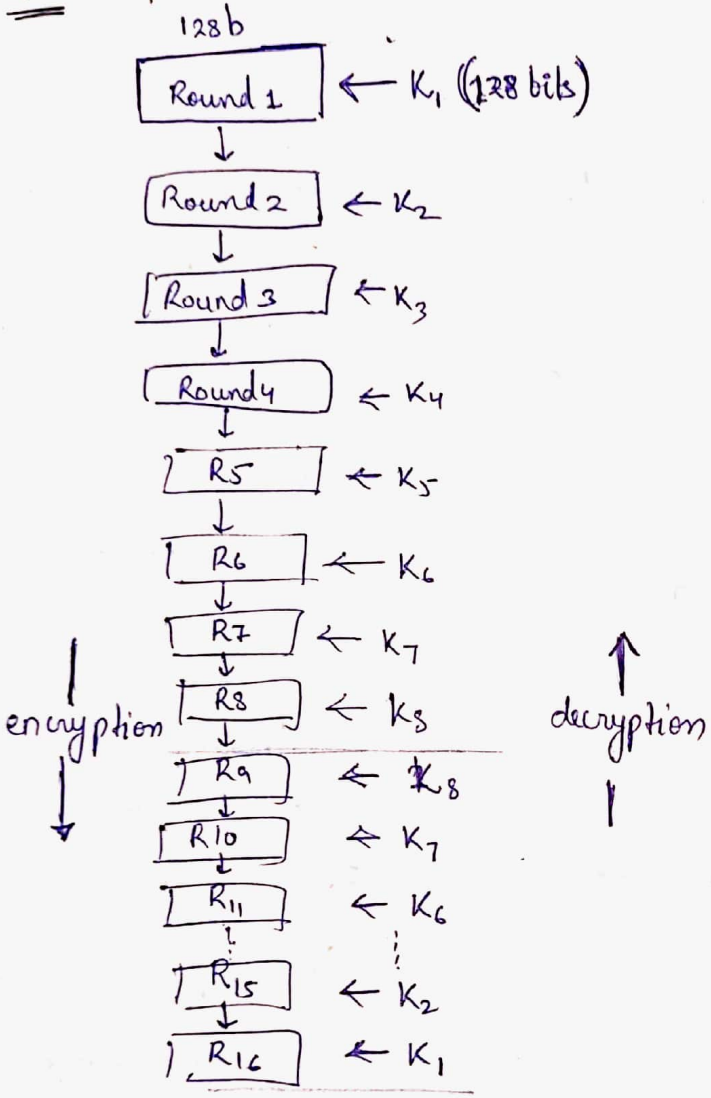
$(b+18) = q*26 + 0$
$b = q*26 - 18$

18, 8, 18

therefore $a=5$, $b=8$ (or 34, 42, 60, ...)

$$c = (5p+8) \bmod 26$$

4.2



The functions used in Rounds 9 through 16 are mirror images of the functions used in Rounds 8 down to 1.

Encryption is done from Round 1 to Round 16 and Decryption is done from Round 16 to Round 1.

From the key schedule, we can see that encryption and decryption are identical.

We are given a ciphertext c. let $m' = c$. Now we will ask the Orcale to encrypt the m'. The ciphertext returned by the oracle will be the decryption of c. i.e our plain text just using one single query to oracle.

4.6

(a) 32-bit string of zero.

$F(R_n, K_{n+1}) = 0$ (n-bit strings of zeroes)

$L_0 = R_0$

$R_1 = L_0 \text{ XOR } F(R_0, K_1) = L_0 \text{ XOR } 0 = L_0$

⋮

$L_{n+1} = R_n$

$R_{n+1} = L_n \oplus F(R_n, K_{n+1}) = L_n \oplus 0 = L_n$

$L_{n+2} = R_{n+1} = L_n$

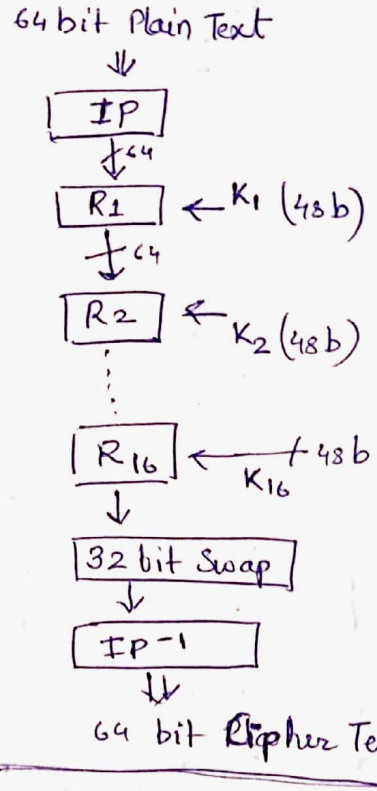
$R_{n+2} = L_{n+1} = R_n$

After every two rounds we obtain original input

Therefore $L_{16} = L_0$, $R_{16} = R_0$

Swap $\Rightarrow$ $R_{16} L_{16} \xrightarrow{IP^{-1}} R_0 L_0$

DES Encryption



Round Structure

$L_i = R_{i-1}$

$R_i = L_{i-1} \text{ XOR } F(R_{i-1}, K_i)$

1.) Therefore, the transformation computed by the modified DES can be represented as follows: $C = IP^{-1}(SWAP(IP(M)))$

2.) Decryption would be similar with $L_{16} \Rightarrow L_0$ & $R_{16} \Rightarrow R_0$

$M = IP^{-1}(SWAP(IP(C)))$

(b) R

$F(R_n, K_{n+1}) = R_n$

$L_1 = R_0$

$R_1 = L_0 \text{ XOR } F(R_0, K_1) = L_0 \text{ XOR } R_0$

⋮

$L_{n+1} = R_n$

$R_{n+1} = L_n \oplus F(R_n, K_{n+1}) = L_n \oplus R_n$

$L_{n+2} = R_{n+1} = L_n \oplus R_n$

$R_{n+2} = L_{n+1} \oplus R_{n+1} = L_{n+1} \oplus (L_n \oplus R_n) = R_n \oplus L_n \oplus R_n = L_n \oplus 0$
$= L_n$

$L_{n+3} = R_{n+2} = L_n$

$R_{n+3} = L_{n+2} \oplus R_{n+2} = (L_n \oplus R_n) \oplus L_n = R_n$

Therefore, after each three rounds, we obtain original input.

$L_{15} = L_0$, $R_{15} = R_0$

$$\begin{cases} L_{16} = R_{15} = R_0 \\ R_{16} = L_{15} \oplus R_{15} = L_0 \oplus R_0 \end{cases}$$

Swap $\Rightarrow$ $R_{16} L_{16} \xrightarrow{IP^{-1}} R_{16} L_{16} \Rightarrow (L_0 \oplus R_0 , R_0)$

1) Transformation can be represented by

$$C = IP^{-1}(F_k(IP(M))) \qquad F_k(A,B) = (A \oplus B, B)$$

2) Decryption would be similar to the encryption. with $L_{16} \Rightarrow L_0$ $R_{16} \Rightarrow R_0$.