Test -1 CNS

Roll no- 21410103l.

Q.S. Avalanche effect & effect in DES -

It states that a single small change is the plain text or message. should have a cascading effect on. entire cipher text generation,

So that the end cipher text is totally different from the first cipher text.

This is a desirable trait is a. encryption algo, thus keys uniquely identify the plain text & authenticity can be verified just using cipher text.

So a small change is iput leads to ~~a~~ big change in output.

In DES we have 16 rounds & 2 permutation.

(2) 21410103 I

In each round, the input bits are used to look up for the output according to function.

Thus a small change in subsequent rounds lead to a totally different end cipher text.

Thus having an avalanche effect.

x —— x —— x —— x ——

Q.3. Yes, a block cipher can be constructed using a hash function.

The feistal structure refers to the same as ~~as~~ said above.

The one half key is used with a hash function on first part of text block.

This than is XORed with the remaining half.

Since it heads the same direction for function both for encryption & decryption.

Thus the hash function can be used in block cipher as explained.

Q.4 A → B $M_1 = M \oplus N_A$ ... (a)

B → A $M_2 = M_1 \oplus N_B$ ... b

A → B $M_2 \oplus N_A$ ... c

a) Recovery for B ⇒

B will have to XOR the later received message with original message.

(4) 2140 01031

$M_2 \oplus N_A \oplus M_1$ .... d

Since M_1 is from (a).

$M_1 = M \oplus N_A$.

Substituting (a) in (d).

We get.

$M_2 \oplus N_A \oplus M \oplus N_A$.

$M_2 \oplus M$.

Also, the message M_2 originated from B.

Thus using M_2 to be XOR'ed.

We have

$M^* = M_2 \oplus M \oplus M_2$

$= \boxed{M}$

Thus B is able to retrive the message M. the given way.

Q. E. D.

b). No, this system is not secure as any one intercepting the messages has access to M_1 & M_2 & $M_2 \oplus N_B$. And. using these the original text can be deciphered as shown.

Thus is system is not safe.

Q.2. Advantages & Disadvantage of S-block in DES.

-> It offeres security as it is non-linear.

-> S-block is just no-linear part which is XOR operations of key, plain text & ciper text.

=>.