Jessica Braganza
BE Comp 2
F17112151

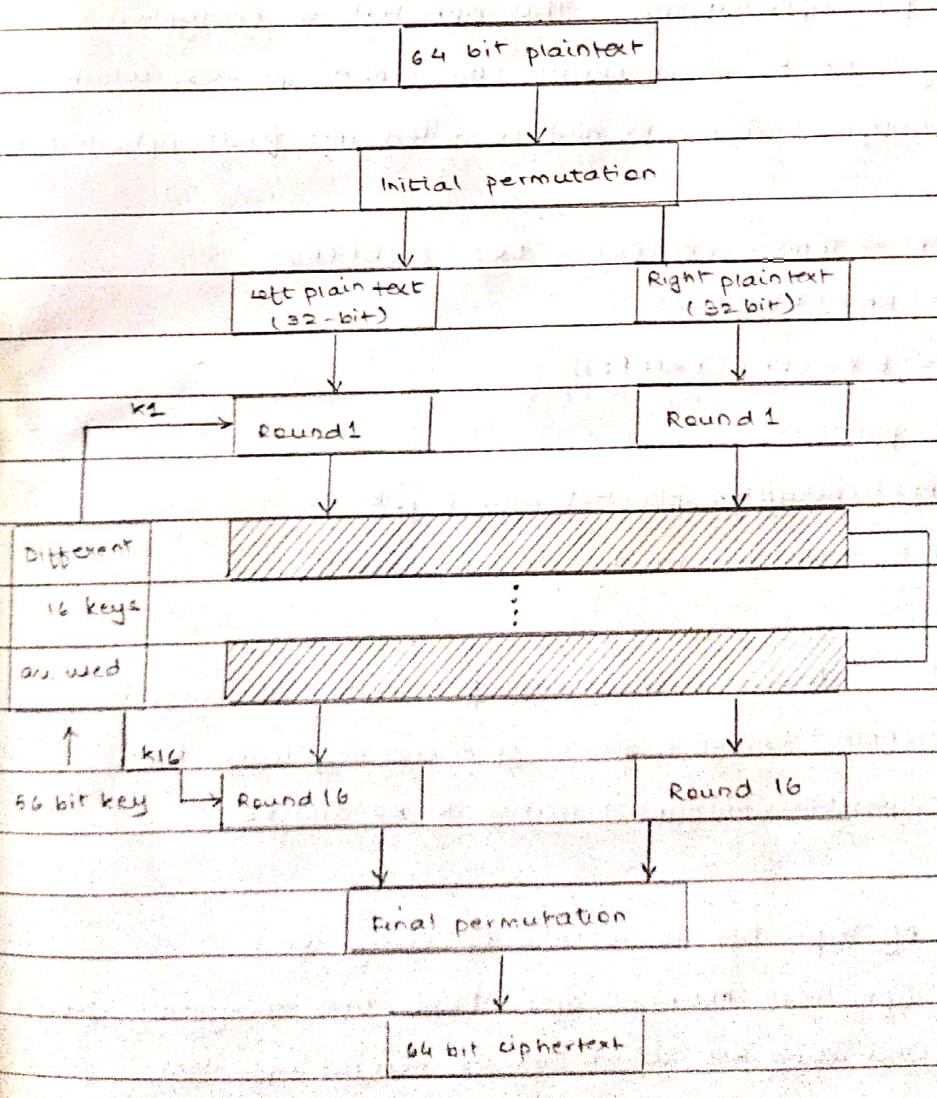
PAGE NO :
DATE :

ICS Assignment 3

1) Explain working of DES in detail.

Ans :- DES is Data Encryption Standard. It takes 64 bit plaintext as an input and creates 64 bit ciphertext i.e. it encrypts data in block of size 64 bits per block. Divide plaintext message into 64 bit block each.

- At the decryption side DES takes 64 bit ciphertext and creates 64 bit plaintext using same 56 bit key.
- The principle of DES is very simple. Divide plaintext message into blocks of size 64 bits each which is initial permutation



- After initial permutation on 64 bit block, the block is divided

into 2 halves of 32 bit called left plaintext and right plaintext.
- The left plaintext and right plaintext goes through 16 rounds of encryption process along with 16 different keys for each round.
- After 16 rounds of encryption process, left plaintext and right plaintext gets combined and final permutation is performed on these combined blocks.

2) Explain triple DES.

Ans - Triple DES performs the same operation as double DES.
- Only difference is that triple DES uses three keys K1, K2 and K3 while encrypting plaintext.
- First it performs encryption on plaintext which is encrypted using K1 obtains first ciphertext, again this ciphertext is encrypted using another key called K2 which obtains the second ciphertext which is again encrypted using K3 and converted into final ciphertext Cp.

Mathematically,

$P \rightarrow E_{K1}(Pt) \rightarrow TEMP = E_{K1}(Pt) \Rightarrow E_{K2}(E(K1(P)))$

$\Rightarrow E_{K3}(E_{K2}(E_{K1}(Pt)))$

$\Rightarrow Cp = E_{K3}(E_{K2}(E_{K1}(Pt)))$

where Pt = plaintext

$E_{K1}(Pt)$ = encrypted plaintext with key K1

TEMP = Temporary variable to store results.

$E_{K2}(E_{K1}(Pt))$ = Encrypted results of first ciphertext using K1

$E_{K3}(E_{K2}(E_{K1}(Pt)))$ = Encrypted results of second step using K2.

Cp = Final ciphertext encrypted using K1, K2 and K3.

- Decryption of triple DES is reverse of encryption.
- The final ciphertext obtained after triple DES encryption process gets decrypted using K3 which results second ciphertext, second ciphertext decrypted using K2 which results first ciphertext, first ciphertext again decrypted using K1 which

generate the original plaintext Pt.

$P_t = DK3(DK2(DK1(C_p)))$

8) What is weak key in DES algorithm? Explain with example.

Ans - Weak keys are the keys that cause the encryption mode of DES to act identically to the decryption mode of DES.

- In operation, the secret 56 bit key is broken up into 16 subkeys according to the DES key schedule, one subkey is used in each of the 16 DES rounds. DES weak keys produce 16 identical subkeys. This occurs when the key is :

i) Alternating ones + zeroes.

ii) Alternating 'F' + 'E'

If an implementation does not consider the parity bits, the corresponding keys with the inverted parity bits may also work as weak keys.:

i) all zeroes ii) all ones.

iii) Using weak keys, the outcome of PC-1 in DES key schedule leads to round keys being either all zeroes, all ones or alternating zero-one patterns.

iv) Since all the subkeys are identical and DES is a Feistel network, the encryption function is self inverting that is despite encrypting once giving a secure looking cipher text, encrypting twice produces the original plaintext.