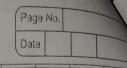
| , | |
|--------|--|
| | Page No. Date |
| 00 | Devanshu Surana |
| | PC-23, Panel C |
| | 1032210753 |
| | Colour la should at it |
| fid Co | 103 Lab A2. La Vida 199 mission - |
| | 30 N Dtol |
| wor | FASISIO otal conidmo- per bowos Alia 90x- |
| 1. | what is the concept of Feistel cipher? |
| Ans. | It is a symmetric-key block cipher structure used in |
| 0 | modern encryption algorithms. It divides the input date into two halves and applies a series of rounds |
| | into two haires and applies a series of rounds |
| onit 3 | where one half is modified based on the other |
| | half and a round key this process is repeated |
| 1 | mumple times, and the two halves are eventually |
| h | swapped or combined to produce the ciphertext. |
| | internally in the DES algorithm. |
| 2. | Draw and describe DES algorithm. tokens |
| | and thirty and the |
| Ans. | Substitution (S-pox) |
| Ans. | Step 1 Plain oftert (64 bits) |
| Ans. | Step 1 (Plain oftert (64) bitse) upor |
| Ans. | Step 1 Plain ontext (64 bits) grade step 2 Initial Permutation (IP) |
| Ans. | Step 1 Step 1 Step 2 Initial Permutation CIP) 279 20 done 20 dold 2 who mand so |
| Ans. | Step 1 Step 1 Step 2 Initial Permutation CIP) Step 3 LPT RPT Methodology Additional Step 1 LPT RPT Methodology |
| Ans. | Step 1 Step 1 Step 2 Initial Permutation CIP) Step 3 LPT RPT Address LAND L |
| Ans. | Step 1 Plain oftert (64 bits) Step 2 Initial Permutation (IP) Step 3 LPT RPT Step 4 Key 16 Rounds 16 Rounds 4 key |
| Ans. | Step 1 Plain oftert (64 bits) Step 2 Initial Permutation CIP) Step 3 LPT RPT RATE OF STEP 4 Step 4 Key 16 Rounds 16 Rounds 4 Key |
| Ans. | Step 1 Plain ontext (64 bits) Step 2 Initial Permutation (IP) Step 3 LPT RPT Step 4 Key 16 Rounds 16 Rounds + key Step 5 Find Permutation (FP) |
| Ans. | Step 1 Plain ontext (64 bits) Step 2 Initial Permutation CIP) Step 3 LPT RPT LPT RPT Step 4 Key 3 I6 Rounds 16 Rounds Fey Step 5 Find Permutation (FP) |
| Ans. | Step 1 Plain ontext (64 bits) Step 2 Initial Permutation (IP) Step 3 LPT RPT Step 4 Key 16 Rounds 16 Rounds + key Step 5 Find Permutation (FP) |
| Ans. | Step 1 Plain ontext (64 bits) Step 2 Initial Permutation CIP) Step 3 LPT RPT LPT RPT Step 4 Key 3 I6 Rounds 16 Rounds Fey Step 5 Find Permutation (FP) |



initial permutation that rearranges the bits acc. to table.

2. 16 Rounds of Processing:

- Expansion, substitution and permutation of 32 bit

- XOR with Round key-combines data with the round subkey.

3. Final Permutation: After the 16 rounds, a final permutedion is applied of the data which is the inverse of initial permutation.

4. Cipher text output: The final output of the final permutation is the appertext.

3. List and state broad-level operations used internally in the DFS algorithm.

Ans. Permutations CIP and FP)

Substitution (S-box)

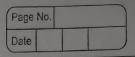
Expansion (Key expansion)

yor operations (bet data and round keys)

4. Compare various block ciphers such as DFS, AES,

Ans. DES CData Encryption Standard):
Uses a 56-bit key, considered insecure for modern standard

AES (Advanced Encryption Standard): Uses key sizes of 128, 192 or 256 bits, highly secure, and widely adopted.



Blowfish: Uses variable length key (32 to 448 bits), known for its speed but not widely used in practice. 5. What are the Block, cipher design guidelines.

Ans The block size should be large enough to prevent attacks that experior statistical pattern in the

plaintext. The s-box used in the cipher should be non-linear to provide confusion

Key sizes should be larger because it resist brute - force attacks.

More rounds increase complexity and security.

