Q1)

Is it possible to construct a hash function to construct a block cipher with a structure similar to DES. Because a hash function is one way and a block cipher must be reversible (to decrypt()). How is it possible?

Ans: Constructing a hash function that create the structure of a block cipher like DES (Data Encryption Standard) is possible, but it involves specific design considerations due to the inherent differences between hash functions and block ciphers.

Example Structure:

- Split the input block into two halves.
- For each round:
  - Use hash function to process one half with a round key
  - XOR the output with the other half.
  - Swap the halves

Q2

Can we use encryption for message integrity? If yes prove it.

Ans: No, we cannot use encryption for message integrity, we use encryption for confidentiality. This is because in encryption we convert the secret message to un-readable format and on the other hand, message integrity is the process in which we ensure that message we receive must be same to the message which source send to us.

Q3

How many keys are used in Tripple DES algorithm? Why is the middle portion of 3-DES a decryption rather than encryption?

Ans: In triple Des we use three keys (K1, K2, K1). Each key of 56 size, hence 56 x 3 = 168 effective key size in triple DES. There is no cryptographic significance of decryption in middle portion.

The middle portion of 3-DES is a decryption step because the algorithm follows an **Encrypt-Decrypt-Encrypt (EDE)** structure. This design allows for backward compatibility with single DES while enhancing security; the initial encryption and final encryption steps use one key, while the middle decryption step uses a different key, effectively adding complexity to the encryption process.

Q4

What are the techniques in Steganography?

Ans:

Character Marking: It is the technique in which the changing letters in message gives a secret message. For example, first letter of each sentence gives a secret message.

Invisible Int: It is the technique in which the secret message is written with the ink that will only be displayed by applying some chemicals or by placing it towards the light.

Pin Punctuations: It is the technique which contains small dots on paper in such a way to gives a secret message.

Typewriter Correction Ribbon: It is the technique in which correction are made in type writer in such a way that it gives a secret message

Q5

How the Round key is generated from the cipher text in AES?

Ans: Here Let's suppose we have a cipher text

2b	28	ab	09			
7e	ae	f7	Cf			
15	d2	15	4f			
16	a6	88	3c			

W_{i-4} W_{i-1} W_i

Root Word

- $W_i = W_{i-1}$ => top shift => Replace with S-boxes => $S[W_{i-1}]$
- $Wi = Wi\text{-}4 \oplus S[W_{i-1}] \oplus \mathrm{RCON}(4)$

Other Words

- $Wi = Wi\text{-}4 \oplus W_{i-1}$

Q5

How redundant data is more helpful for cryptanalysis?

Ans: Redundancy in data can be helpful in cryptanalysis in several ways:

1) **Repeated Patterns:**
   Redundant data can reveal patterns or repetitions, which cryptanalysts can exploit to break encryption. If certain pieces of data appear multiple times, it may provide clues about the underlying structure of the cipher.
2) **Statistical Analyst:**
   Cryptanalysts can use statistical methods on redundant data to analyze frequency distributions of characters or bytes.
3) **Error Detection:**
   Redundant data allows for error detection and correction.

Q6

Write down the design principles of block ciphers to make DES more resistant to linear and differential cryptanalysis?

Ans: To make the Data Encryption Standard (DES) more resistant to linear and differential cryptanalysis, several design principles can be applied to block ciphers.

1. **Increased Number of Rounds**: Increasing the number of rounds in the encryption process enhances security.
2. **Non-linear S-Boxes**: The S-boxes (substitution boxes) used in the encryption process should be highly non-linear. This non-linearity helps to obscure the relationship between the plaintext and ciphertext, making it difficult for attackers to use linear approximations effectively.
3. **Avalanche Effect**: The design should ensure that a small change in either the plaintext or the key results in a significant change in the ciphertext.

4. **Key Schedule Complexity**: The key schedule, which generates round keys from the main key, should be designed to ensure that each round key is independent and unpredictable.