1	a) Discuss the historical facts of cryptography. How it has matured to the modern cryptography. What are the key milestones in this journey. b) Discuss few attacks on the block ciphers with proper diagram and example.
2	Define and elaborate following terms about cryptography a) Trapdoor Functions b) RSA Trapdoor permutation c) Simple Attack on textbook RSA d) Diffie-Hellman Protocol e) Modular Inversion f) Dlog in $(Z_p)^*$ g) Factoring Problem h) Modular e'th Roots
3	a) Merkle Puzzles were supposed to be a good idea but later there were various attacks on this. Discuss Merkle Puzzles with example. b) Chosen cyphertext attacks are very powerful in nature. Discuss Chosen ciphertext attacks with example and diagram in context with authenticated encryption.
4	How message integrity can be maintained. What are the main issues with the message integrity? Also give possible attacks and their solutions.
5	Write short notes on the following a) What is the current status of DNA Cryptography Technology? b) What are the applications of Elliptic Curve Cryptography? c) Discuss the advantages of Quantum Cryptography. d) Explain and differentiate Digital water marking and steganography.