Question Bank for CIE-1

1. Briefly explain the block cipher modes of operations? –[10M]
2. Explain the key expansion function of AES algorithm---[6M]
3. Explain the RSA algorithm and steps of algorithm? Give an example of encryption and decryption using RSA? —[10M]
4. Differentiate between: [10M]
   i) Block Cipher and Stream Cipher
   ii) Monoalphabetic and polyalphabetic ciphers

5. Differentiate between DES and AES algorithms. [6M]
6. Explain the Play Fair cipher algorithm? Encrypt the message 'MYBALLOON' using the key 'MONACHRY'—[8M]

7. Generalize the security services classifications and security mechanisms in detail. [8M]
8. Explain the requirements of public key cryptography [6M]
9. Given p=19, q=23, and e=3 Use RSA algorithm to find n, Φ (n) and d.
10. What are the Applications of Public Key Cryptosystems---[4M]?
11. Explain in detail Feistel encryption and Decryption algorithm. [10M]
12. Illustrate Strength of DES algorithm.
13. Explain all the four transformations by using AES diagram for each round. —[8M]
14. Illustrate public key cryptosystems for Authentication and Secrecy. —[8M]
15. Explain the Security Attacks-Active and Passive attack types in detail—[10M]
16. With a neat diagram explain the simplified model for conventional encryption with its components—[10M]
17. Explain Caesar cipher and encrypt the following text "Attack At Seven" ----[5M]
18. What is Avalanche Effect? Explain with an example------------[4M]
19. List out AES parameters------[3M]
20. What is Double DES and Triple DES, Explain—[6M]
21. Given p=7 and q=17, PT(Plaintext)=6, Find the value of e, d to form a public key and private key. What will be the Cipher text and again calculate text value from cipher text. —[10M]