Information and network security (2170709)
Assignment 1

1. Explain Security Services.
2. Define the terms threat and attack.What is the difference between passive and active security threats? List and briefly define categories of passive and active security attacks.
3. What is symmetric key cryptography? What are the challenges of symmetric key cryptography? List out various symmetric key algorithms and explain Caesar cipher in detail.

4. Explain generation of encryption matrix in play fair cipher.
5. Write differences between substitution techniques and transposition techniques.
6. Explain rail fence Cipher technique.
7. Use Hill cipher to encrypt the text DEF. The key to be used is

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 8 & 7 \end{bmatrix}.$$

8. Explain one time pad cipher with example.
9. Define the term cryptanalysis. Explain various types of cryptanalytic attacks
10. With example explain function of s-box in DES.
11. Explain avalanche effect in DES and discuss strength of DES in brief.
12. Define the term – confusion, diffusion.
13. Explain DES key generation process in detail.
14. Explain single round of DES algorithm.
15. Explain the feistel structure?
16. When an encryption scheme is said to be unconditionally secure and computationally secure?
17. Explain various steps of AES in short.
18. Explain Modes of Operations
19. Explain triple DES with two keys.

Information and network security (2170709)
Assignment 2

1. Explain RSA algorithm with example.
2. Elaborate various kinds of attacks on RSA algorithm
3. What is primitive root? Explain Diffi-Hellmen key exchange algorithm with proper example. Is it vulnerable to man inthe middle attack? Justify.
4. The encryption algorithm to be used is RSA. Given two prime numbers 11 and 3 and public key (e) is 3. Calculate the decryption key and Calculate the ciphertext if the given plaintext is 7.
5. What is digital signature? Explain its use with the help of example.
6. Only Hashing dose not ensures integrity of message in network communication" – Justify your answer with suitable example
7. What is PKI? What are the components of PKI? Explain Certificate Authority in detail
8. Explain key distribution using KDC.
9. What is MAC? Explain HMAC.
10. How following can be achieved with message authentication code(MAC)?
    a. Message authentication
    b. Message authentication and confidentiality
11. Explain authentication mechanism of Kerberos.
12. Explain use and concept of dual signature in SET.
13. Write a short note on "Digital Signature Algorithm"
14. Explain Diffie - Hellman key exchange algorithm
15. Differentiate between hashing and encryption. What are the practical applications of hashing ? Compare MD5 and SHA1 hashing algorithms.
16. Write a short note on SSL.
17. Write a short note on Pretty Good Privacy (PGP).
18. Write a short note on IP security.
19. What is the purpose of X.509 standard