Subject: - Information and Network Security

1. Describe Rail-fence cipher algorithm with example.
2. Explain cryptanalytic attacks with example of any encryption algorithm. 3. Explain one time pad algorithm with example and mention its strength and weakness 4. Draw Generic Model of Digital Signature Process.
5. Describe MAC with its security implications.
6. Explain Schnorr Digital Signature Scheme.
7. Explain use of Public-Key Certificate with diagram and draw X.509 certificate format.
8. Explain Elgamal Digital Signature Scheme
9. Explain working of Secure Hash Algorithm, with basic arithmetical and logical functions used in SHA.
10. What is the role of a compression function in a hash function?
11. Explain process of encryption in RSA Algorithm with suitable example. (Prime Number P,Q and Encryption Key E is given for reference) P=7, Q=17, E=7
12. Perform encryption in Playfair Cipher algorithm with plain text as "INFORMATION AND NETWORK SECURITY", Keyword is "MONARCHY". (Note: 1.Put j and i both combine as a single field in 5*5 matrix).
13. Encrypt the Message "Surgical Strike" with key "GUJAR" using PLAYFAIR technique 14. Distinguish between Symmetric encryption and Asymmetric encryption using suitable example.
15. Explain Avalanche Effect.
16. Discuss Man in Middle Attack.
17. Discuss HASH function and its application in Crypto System.
18. Discuss clearly Secure Hash Algorithm with its real time application.
19. What is KDC? List the duties of a KDC.
20. Discuss HASH function and its application in Crypto System.
21. Explain the difference between diffusion and confusion.
22. Explain in detail RSA algorithm, highlighting its security aspect.
23. Discuss Man in Middle Attack.
24. Discuss in detail encryption and decryption process of DES.
25. Distinguish between Symmetric encryption and Asymmetric encryption using suitable example.
26. Describe the term: Authentication, Authorization, Integrity and Non – repudiation.
27. For what purpose Secure Shell(SSH) is useful? Briefly define SSH protocol. 28. What is the purpose of X.509 standard? How is an X.509 certificate revoked? 29. Define the parameters that define SSL session state and session connection.

30. How cryptanalyst can exploit the regularities of the language? How digrams can solve this problem? Use the key “hidden” and encrypt the message “Message” using playfair cipher
31. Explain Counter (CTR) algorithm mode with diagram.
32. Define following principles of security: 1) Confidentiality 2) Integrity 3) Availability
33. What are the essential ingredients of a symmetric cipher?
34. Discuss the following block cipher modes of operation in detail with neat sketches: - Cipher block chaining mode - Counter mode
35. Enlist the practical applications of hashing.
36. List the requirements of Public Key Cryptography
37. Explain HTTPS in brief.
38. Briefly discuss the working of SSL Record Protocol.
39. Elaborate any one approach to Digital Signatures.
40. Briefly discuss web security threats