1. Ceaser Cipher
2. Monoalphabatic Cipher
3. Playfair Cipher
4. Hill Cipher
5. Vigenere Cipher
6. Vernam Cipher (One-time pad)
7. Transposition Cipher (Rail Fence, Single Column, and Double Column Ciphers)
8. Affine Cipher
9. Euclidean Method for Determining GCD (Integer and Polynomial Both)
10. Extended Euclidean Method for Determining Multiplicative Inverse (Integer and Polynomial Both)
11. Active and Passive Attacks
12. Block Cipher Vs. Stream Cipher
13. Feistel Cipher
14. Shannon’s S-P Networks (Diffusion and Confusion)
15. Assignment last 2 questions
16. Simplified-DES, DES, 2DES and 3DES, Meet-in-Middle Attack in 2DES
17. Finite Field (Groups, Rings, Fields)
18. AES (AES Structure, AES Round Function, AES Key Expansion, AES Decryption, AES S-box Design)
19. Block Cipher Modes of Operations
20. Asymmetric or Public Key Cryptosystem with Suitable Diagrams
21. RSA Algorithm with Numerical
22. Diffie Hellman Key Exchange + El Gamal Cryptosystem with Numerical
23. MAC, CMAC and HMAC
24. Hashing Functions: MD5 and SHA-5 12, SHA-1
25. Digital Signature Algorithm (RSA Approach and Digital Signature Standard)
26. Euler Totient Function, and Fermat Little Theorem with Examples
27. Kerberos (An Authentication Application)
28. Intrusion Detection System

(NIDS & HIDS with Pros and Cons, Signature Based Detection Process, Anomaly Based Detection Process)

1. IP Security (ESP and AH)
2. Secure Socket Layer (Open SSL)
3. Fundamentals of Firewall