

1. What is cryptanalysis and cryptography?
2. What are the types of attacks on encrypted message?
3. What are the key principles of security?
4. Compare Substitution and Transposition techniques with Example.
5. What is Caesar cipher? How to Encrypt a message "Cryptography" with key 3 using Caesar cipher?
6. How does simple columnar transposition work?
7. What is Monoalphabetic cipher? How it is different from Polyalphabetic cipher?
8. Compare stream cipher and block cipher with example.
9. Compare Substitution and Transposition techniques.
10. What is the difference between diffusion and confusion?
11. How many keys are required for two people to communicate via a cipher?
12. Draw the general structure of DES and explain the encryption decryption process.
13. What is AES? Draw the general structure of AES and explain the encryption decryption process.
14. Mention the strengths and weakness of DES algorithm.
15. Find $\gcd(56, 86)$ using Euclid's algorithm.
16. Define Fermat Theorem.
17. Define Euler's theorem and its application.
18. How to calculate Euler's phi value of any number?
19. Perform encryption and decryption using RSA Algorithm. for the following.
 $P=7; q=11; e=17; M=8$.
20. Perform decryption and encryption using RSA algorithm with $p=3, q=11, e=7$ and $M=5$.
21. Discuss any two Asymmetric Technique and list their merits and demerits.
22. User A and B exchange the key using Diffie-Hellman algorithm. Assume $\alpha=5, q=11, X_A=2, X_B=3$.
Find the value of Y_A, Y_B and k .
23. What is MAC.
24. What is Hash Function
25. Define SHA-1
26. Write and explain the digital signature algorithm.
27. What are the properties a digital signature should have?
28. What are the characteristics of good Password?
29. What IP security?
30. What is Web security?
31. What is Firewall?
32. What are the function areas of IP security?
33. What are the positive and negative effects of firewall?
34. Explain the architecture of IP Security
35. What you understand by Malicious Software. How it's harm to computer
36. List and Brief, the different generation of antivirus software
37. Explain the security with antivirus software.