**Cryptography 2022-2023 Assignment, Branch : CSE**

Q1. What is meant by cryptography? Write about security services and security mechanisms in cryptography.

Q2. Discuss the various principles involved in private and public key cryptography.

Q3. Write briefly about the attacks? What are the x.800 listed attacks?

Q4. Discuss the key distribution technique in cryptography.

Q5. What is a Fiestel Cipher? Name the Ciphers that follow fiestal Structure.

Q6. Explain about Hill Cipher. Consider the plaintext “paymoremoney” and use the encryption key : K =. Find the cipher text.

Q7. How is key expansion done in Blowfish?

Q8. Describe about IDEA encryption and decryption. Write the applications which  
use IDEA.

Q9. Distinguish between diffusion and confusion. Explain Data Encryption standard (DES) in detail.

Q10. Explain Advanced Encryption System (AES) cipher in detail.

Q11. What are Confusion and Diffusion properties of Modern Ciphers?

Q12. Explain about Euclidean algorithm for Greatest Common Divisor.

Q13. Explain the Fermat’s theorem?

Q14. Define Euler’s theorem and list out its applications.

Q15. What is Eulers Totient function? Find it for 37 and 21.

Q16. What is addition, multiplication and multiplicative and additive inverses modulo 8?

Q17. Solve the congruence x5≡11 mod 17.

Q18 Find the value of φ( 100) and φ ( 80)

Q19. Describe RSA algorithm and estimate the encryption and decryption value for the RSA algorithm parameters.

Q20. What is the cipher text if the plain text is 63 and public key is 13? Use RSA algorithm.

Q21. Write short notes on Digital Signature Algorithm

Q22. Briefly explain the Diffie Hellman Key Exchange algorithm? Let q=353 and α=3. Xa=97, Xb=233. Use Diffie Hellman Key exchange algorithm to find Ya, Yb and Secret key K.

Q23. What is message authentication? How is it different from message integrity?

Q24. What is the requirement of cryptographic Hash functions?

Q25. What is the difference between Hash function and Message Authentication Code?

Q26.Give the structure of SHA-512 compression function. Explain the structure of  
each round. Is Man in the Middle attack possible on SHA-512

Q27. with a neat flow chart, Show how MD5 process a single 512 bit block.

Q28. Differentiate digital signature from digital certificate.

Q29. Give a brief notes on X.509 authentication services.

Q30. Explain Kerberos version 4 in detail?

Q31. How does PGP provide authentication and confidentiality for email services and  
for file transfer applications? Draw the block diagram and explain the components.

Q32. Describe the architecture of IPSec.

Q33. Draw the IP security authentication header and describe the functions of each field.

Q34. Explain web security threats and security approach.

Q35. Explain Secure socket layer in details?

Q36. Explain transport layer security in details?

Q37. Explain secure electronic transaction with neat diagram..

Q38. What is session hijacking in cyber security?

Q39. What is intruders. Explain different intrusion technique.

Q40. Explain about Intruder detection system (IDS)?

Q.41 What are the password selection strategies?

Q42. Explain about malicious programs in computer . Write antivirus approach to protect our system from malicious programs**.**

Q43. Differentiate between computer Virus and Worms with two examples each.

Q44. What is firewall. Explain different types of firewall and mention the layer in which they operate.

Q45. Explain the configuration of firewall in detail.

Q46. Write short notes on :

(i) man in the Middle Attack. (ii) avalanche effect (iii) replay attack (iv) phishing attack

(v) IP Spoofing (vi) ARP poisoning (vii) computer virus (vii) SQL injection attack