K J Somaiya Institute of Engineering and Information Technology

An Autonomous Institute Affiliated to University of Mumbai

Department of Computer Engineering
CSS Sem VI
Academic Year 2021-2022

1. Explain the security model with block diagram
2. Explain following terms:
    a. Access control, Non-repudiation Authorization, Confidentiality, Integrity
3. Difference between authorization and authentication
4. Numerical on totient function, GCD, Fermat’s theorem and Euler’s theorem.
5. What are different security services
6. Explain different types of attacks with example
7. What are different security techniques
8. What are different security mechanisms
9. Apply transposition cipher to encrypt and decrypt the message ------.
10. Apply Hill cipher to encrypt the message “----”. The key for encryption is “------”. And decrypt the encrypted message.
11. Explain symmetric and asymmetric encryption techniques. Explain the various components of symmetric and asymmetric encryption.
12. Compare AES and triple DES in terms of type of algorithm, key length, rounds and resource consumption
13. Explain difference between stream cipher and block cipher
14. What is public key encryption. Give characteristics of public key encryption.
15. How secrecy and authentication is achieved in public key encryption?
16. List strength and weaknesses of the public key.

1. Explain RC4 algorithm in detail
2. Explain DES algorithm in detail
3. Explain AES algorithm in detail
4. Explain Needham-schroeder protocol
5. Explain Kerberos authentication protocol

6. Explain Digital Certificate X.509
7. Compare SHA-1 and MD5
8. Explain MAC
9. Explain CMAC in detail
10. Explain MD5 in detail
11. Explain SHA-1 in detail
12. What is digital signature. Explain in any digital signature. algorithm.
13. What are the different attacks in digital signature?
14. Explain RSA digital signature scheme .
15. What are different methods of authentication. Explain each in brief.
16. What is packet sniffing? Explain with example.
17. What is ARP spoofing? Explain with example.
18. What is port scanning? Explain with example.
19. What is IP spoofing? Explain with example.
20. Explain OSI model layer-wise vulnerability
21. What is the need of SSL? Explain all phases of SSL handshake protocol in detail.
22. What are different viruses and worms? How do they propagate.
23. Write short note on buffer overflow attack.
24. Write short note on SQL injection attack. How it can be prevented?

Subject Teacher

Dr. Shyamal Virnodkar