THIS PIECE OF STUDY MATERIAL HAS BEEN BROUGHT TO YOU BY

# MUSTUDENTS UNITED

*contributed by -* **MU ADMIN**

*of college -* **MU ADMIN**

# SEM 5 IT CNS QB

**10 Marks questions**

1. Explain the need of Network Access Control in Enterprise Network? Explain Major NAC Enforcement methods
2. Explain in detail with Diagram. How Kerberos can be used for authentication.
3. How does IPSec help to achieve authentication and confidentiality? Justify the need of AH and ESP
4. Define Malware. Explain types of Malware. Virus vs Worms.
5. Explain Firewall, Its types ,its advantages and disadvantages
6. Explain different modes of operation of block cipher
7. Explain classical encryption techniques with examples
8. Explain Public Key Cryptography and RSA algorithm. Given modulus n=91 and public key e=5, find the value of p, q, phi(n) and d using RSA. Encrypt M=25.
9. Playfair cipher with example
10. State firewall design principles and its types with advantages.
11. Explain the working of IPsec in its different modes
12. Describe different types of protocol offered by SSL.
13. What is Network Management Security? Explain SNMP V3
14. Explain IDS and its types in detail
15. Explain the OSI Security Architecture and Network Security Model.
16. Explain Email security process. Explain how S/MIME can be used for Digital Signature and verification operations on email messages.
17. Explain the implementation of Network Access Control with one use case
18. Explain different types of denial of service attacks
19. Given modulus n=221 and public key e=7 find the values of p,q,phi(n) and d using RSA encrypt M=5
20. Design sample digital certificate and explain each field of it
21. Show how a Kerberos protocol can be used to achieve single sign on in distributed systems
22. Encrypt ”This is the Final Exam ” with Playfair Cipher , key is ‘Guidance’
23. What is PKI? Explain PKI architecture
24. Explain transposition cipher with illustrative example
25. Given a 5x5 grid and the keyword "PLAYFAIR", encrypt the message "HIDE" using the Playfair cipher. Demonstrate the steps and the final ciphertext.
26. Explain the working of SHA-256 using suitable example.
27. What is a SPAM? Explain different types of SPAMs.
28. What is the significance of IPSec? Explain the different modes of operation in IPSec?
29. Explain the various use cases of NAC.
30. What are the steps involved in implementing NAC solutions?

**5 Marks questions**

1. Explain the CIA triad.
2. Explain the structure and purpose of an X.509 digital certificate.
3. What is the purpose Trojan horse and backdoor.
4. Explain the working of a Virtual Private Network (VPN) and its security benefits.
5. HMAC and CMAC
6. S/MIME
7. RSA Algorithm
8. OSI Security Architecture
9. HTTPS
10. Kerberos
11. Enlist security goals. Discuss their significance
12. Compare and contrast DES and AES.
13. SHA provides better security than MD5 Justify
14. Explain the purpose of keylogger and rootkit
15. Distinguish between passive and active security attacks
16. Differentiate between virus and worm
17. Write short note on :Email Security
18. Explain SSH protocol stack in brief
19. Describe RC5 algorithm with an example.
20. Explain Playfair Cipher with an example.
21. Explain how VPN can be used to encrypt your personal data
22. Firewall design principles
23. Block Cipher Modes of Operation
24. Steganography and its applications
25. SHA 256 and SHA 512
26. SSL Architecture
27. Explain Security Services and mechanisms to implement it.
28. Explain SSH protocol stack in brief
29. A secure e-voting system is to be designed. Discuss the security goals that must met and enlist mechanisms for the same.
30. Enlist properties & applications of Hash function.
31. Explain principle elements of NAC
32. Use cases for NAC
33. Digital Signature