Reg. No.

Question Paper Code	13950

B.E. / B.Tech. - DEGREE EXAMINATIONS, NOV / DEC 2025

Seventh Semester

Computer and Communication Engineering

20CCPW701 - CRYPTOGRAPHY AND NETWORK SECURITY WITH LABORATORY

Regulations - 2020

Duration: 3 Hours Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)

Answer ALL Questions

Marks K – Level CO

1. Steganography aims to hide information in a way that is _____ *1 K1 CO1*
(a) easily detectable (b) inaccessible (c) concealed (d) visible

2. Identify the factor that influences the strength of a cryptographic key: *1 K1 CO1*
(a) Key range and key size (b) Number of network users
(c) Speed of the algorithm (d) Size of the ciphertext

3. Stream ciphers like RC4 are known for: *1 K1 CO2*
(a) Encrypting data in fixed-size blocks
(b) Encrypting data one bit or byte at a time
(c) Being less efficient for encrypting large data streams
(d) Generating multiple keys for each block

4. Select the correct statement about the Blowfish encryption algorithm: *1 K2 CO2*
(a) It uses a fixed 64-bit key size
(b) It is vulnerable to linear cryptanalysis
(c) It allows variable key lengths ranging from 32 to 448 bits
(d) It requires large memory resources

5. In the Knapsack Algorithm, what is the main computational problem that provides its security? *1 K1 CO3*
(a) Finding the sum of subsets of integers (b) Factoring large prime numbers
(c) Solving linear equations (d) Computing modular inverses

6. Public Key Cryptosystems are commonly used to create: *1 K1 CO3*
(a) Encrypted messages (b) Digital signatures (c) Symmetric keys (d) Hash values

7. In MD5, the process block divides the 512 bits into _________ sub blocks. *1 K1 CO4*
(a) 16 (b) 24 (c) 32 (d)84

8. The __________ criterion states that it must be extremely difficult or impossible to create the message if the message digest is given *1 K1 CO4*
(a) One-wayness (b) Weak collision resistance
(c) Strong-collision resistance (d) All of the Mentioned

9. A digital signature ensures what in the context of PKI? *1 K1 CO5*
(a) Confidentiality of the message (b) Integrity and authenticity of the message
(c) Symmetric encryption of the message (d) Faster transmission of data

10. Which of the following techniques is least likely to be used by a firewall to prevent IP spoofing? *1 K1 CO6*
(a) NAT (Network Address Translation)
(b) Deep packet inspection to analyze payload data
(c) State full packet inspection
(d) Packet filtering based on source and destination IP addresses

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

11. Differentiate active attack and passive attack. *2 K2 CO1*

12. Convert the Given Text “CRYPTOGRAPHY” into cipher text using Rail fence Technique. *2 K2 CO1*

13. Why is the middle portion of 3DES a decryption rather than encryption? *2 K2 CO2*

14. Define Diffusion & Confusion. *2 K1 CO2*

15. List the different approaches to attack the RSA algorithm. *2 K1 CO3*

16. What is the objective of the Knapsack problem? *2 K1 CO3*

17. Mention the significance of signature function in DSS approach. *2 K1 CO4*

18. How Digital signature differs from authentication protocols? *2 K2 CO4*

19. Interpret the term message digest and its significance in security mechanisms. *2 K1 CO5*

20. Explain the role of a Certificate Authority (CA) in Public Key Infrastructure (PKI). *2 K2 CO5*

21. State the difference between threats and attacks. *2 K1 CO6*

22. Give the advantages of intrusion detection system over firewall. *2 K1 CO6*

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23. a) Explain classical encryption techniques with an example. *11 K2 CO1*

OR

b) Discuss the components and model of the OSI security architecture. *11 K2 CO1*

24. a) Explore in detail the one-round process of DES encryption and its functionalities. *11 K2 CO2*

OR

b) Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example. *11 K2 CO2*

25. a) Suppose Alice and Bob use an Elgamal scheme with a common prime q = 157 and a primitive root a = 5. If Bob has public key YB = 1 0 and Alice chose the random integer k = 3, what is the cipher text of M = 9? If Alice now chooses a different value of k so that the encoding of M = 9 is C = (25, C2), what is the integer C2? *11 K3 CO3*

OR

b) Alice and Bob use the Diffie-Hellman key exchange technique with a common prime
q = 23 and a primitive root a = 5.
i. If Bob has a public key YB = 10, what is Bob's private key YB?
ii. If Alice has a public key YA = 8, what is the shared key K with Bob?
iii. Show that 5 is a primitive root of 23. *11 K3 CO3*

26. a) Illustrate the working steps of SHA-512 using a block diagram. *11 K2 CO4*

OR

b) Summarize CMAC algorithm and its usage. *11 K2 CO4*

27. a) Explain the sequence of message exchanges in Kerberos Version 4. Summarize the purpose of each step in the authentication process. *11 K2 CO5*

OR

b) Present an overview of approaches to public-key distribution. Analyze the risks involved in each approach. *11 K2 CO5*

28. a) Describe the operational process of PGP. *11 K2 CO6*

OR

b) Explain the Intrusion Detection System in detail with a suitable diagram. *11 K2 CO6*