**(NO.OF PAGES:2)**

**21PCS312**

**FOR THE CANDIDATES ADMITTED DURING THE ACADEMIC YEAR 2021 ONLY)** **REG.NO**

**NGM COLLEGE (AUTONOMOUS) POLLACHI**

**END-OF-SEMESTER EXAMINATIONS: DECEMBER-2022**

**M. Sc-Computer Science** **MAXIMUM MARKS: 70**

**III SEMESTER** **TIME: 3 HOURS**

# NETWOK SECURITY AND CRYPTOGRAPHY

## SECTION – A (10 X1 = 10 MARKS)

**ANSWER THE FOLLOWING QUESTIONS**
**MULTIPLE CHOICE QUESTIONS (K1)**

1. A loss of _____is the unauthorized modification or destruction of information.
   a) Integrity b) availability
   c) confident ability d) Authenticity

2. Original message is termed as ___ and coded message is termed as _____.
   a) Plain text , cipher text b) cryptotext, plain text
   c) single key text, plain text d) double key text, plain text

3. Let A's public key is n=6, 736, 180, 7817, 961, 456, 267 and e = 5 and B sends the ciphertext. c = 456, 871, 122, 391, 882, 538 to A. Determine B's message in numeric format?
   a) 235813 b) 57971.89 c) 770190.04 d) 687651.9

4. _____ is a mechanism or service used to verify the integrity of a message
   a)Message encryption b) message Decryption
   c) message authentication d) message digest

5. Network access server (NAS) functions as an access control point for users in remote locations connecting to an enterprise's internal network also called a _____.
   a) media gateway b) a remote access server (RAS)
   c) policy server d) All the above

**ANSWER THE FOLLOWING IN ONE (OR) TWO SENTENCES (K2)**

6. Define Security attack
7. Explain block cipher.
8. Define cipher text.
9. List the four elements involved in Ellipitcal Curve Digital Signature.
10. Whai id Firewall?.

**(CONTD…2)**

**SECTION – B (5 X 4 = 20 MARKS)**

**ANSWER EITHER (a) OR (b) IN EACH OF THE FOLLOWING QUESTIONS. (K3)**

11. a) Elucidate various security attacks.

**(OR)**

b) Examine the Relationship Between Security Services and Mechanisms.

12. a) Assess the different types of attacks on encrypted messages.

**(OR)**

b) Compare and construct Stream cipher and block cipher.

13. a) Differentiate Conventional Encryption and public key encryption

**(OR)**

b) List the requirements that a public key cryptosystems fulfill to be a secure algorithm.

14. a) Examine Applications of Hash Functions in brief.

**(OR)**

b) Illustrate the Signature authentication process in ECDSA algorithm.

15. a) Summarize S/MIME and its four principal services provided by S/MIME?

**(OR)**

b) Outline the features of web security.

**SECTION – C (4 X 10 = 40 MARKS)**

**ANSWER ANY FOUR OUT OF SIX QUESTIONS.**
**(16TH QUESTION IS COMPULSORY AND ANSWER ANY THREE QUESTIONS FROM Q.NO: 17 TO 21 ) (K4) OR (K5)**

16. Illustrate the model of network security with neat diagram.
17. Design the Attack tree for internet banking authentication.
18. What is Steganography? Analyse its principle in Network security.
19. Examine the different approaches to attack the RSA algorithm.
20. Elucidate Hash function based on cipher block chaining and SHA algorithm
21. Outline Transport Layer Security.