Regd. No. | | | | | | | | | | |

VIGNAN'S
Foundation for Science, Technology & Research
(Deemed to be University)
-Estd. u/s 3 of UGC Act 1956

Regulation: R13 **Code No: CS427/11**

IV B. Tech I Semester Supplementary Examinations – June 2019

CRYPTOGRAPHY AND NETWORK SECURITY

(CSE/IT)

Time: 3Hrs **Max. Marks: 60M**

SECTION – A

Answer all ten questions **10×1M=10 M**

1. Give any four names of substitution techniques
2. How many keys are required for two people to communicate via a cipher?
3. What is the purpose of the Sub Bytes?
4. What primitive operation is used in RC4?
5. What are the properties a digital signature should have?
6. What are the requirements of the hash function?
7. What is X.509 Standard?
8. Specify the IP security services.
9. What is application level gateway?
10. What do you mean by a trusted system?

SECTION – B

Answer all five questions **5×2M= 10 M**

11. Define Steganography.
12. List four general characteristics of schema for the distribution of the public key.
13. What is goal of PGP.
14. What is the role of Ticket Granting Server in inter realm operations of Kerberos?
15. Give IPSEC ESP Format.

SECTION – C

Answer all four questions **4×5M= 20 M**

16. Describe the various security mechanisms

(OR)

17. Explain shortly on Symmetric Cipher Mode

18. Explain public key cryptosystem.

(OR)

19. Describe the MD5 message digest algorithm with necessary block diagrams.

20. Explain RSA algorithm in detail, perform encryption and decryption to the system with p=7, q=11, e=17 and M=8.

(OR)

21. Explain digital signature standard.

22. Discuss about X.509 authentication service in detail

(OR)

23. Explain briefly about IP Security architecture.

SECTION – D

Answer all two questions **2×10M= 20 M**

24. Draw the general structure of DES and explain the encryption decryption process.

(OR)

25. Describe about RC4 algorithm

26. Explain the types of Host based intrusion detection. List any two IDS software available.

(OR)

27. Describe the familiar types of firewall configurations