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

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

Regulation: R13 **Code : CS427/7**

IV B.Tech I Semester Regular Examinations – November, 2018

CRYPTOGRAPHY AND NETWORK SECURITY

Time: **3** hours (CSE / IT) Max. Marks: **60**

SECTION – A

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

1. We use Cryptography term to transforming messages to make them secure and immune to.
   a) Change b) Idle c) Attacks d) Defend
2. Shift cipher is sometimes referred to as the
   a) Caesar cipher b) Rotor c) cipher d) cipher text
3. Advanced Encryption Standard (AES), has three different configurations with respect to number of rounds and
   a) Data Size b) Round Size c) Key Size d) Encryption Size
4. Triple DES
   (i) is a symmetric key encryption method
   (ii) guarantees excellent security
   (iii) a public key encryption method with three keys
   (iv) is implementable as a hardware VLSI chip
5. Which one of the following algorithm is not used in asymmetric-key cryptography?
   (i) RSA algorithm (ii) diffie-hellman algorithm
   (iii) electronic code book algorithm (iv) none of the mentioned
6. Two way authentication is
   (i) Double transfer of information (ii) No transfer of information
   (iii) Half duplex transfer of information (iv) None of the above
7. Pretty good privacy (PGP) is used in
   (i) browser security (ii) email security (iii) FTP security (iv) none of the mentioned
8. In tunnel mode IPsec protects the
   (i) Entire IP packet (ii) IP header (iii) IP payload (iv)None of the mentioned
9. A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as ……
   (i) Chock point (ii) meeting point (iii) firewall point (iv) secure point
10. Which of the following is a type of program that either pretends to have, or is described as having, a set of useful or desirable features but actually contains damaging code.
    (i) Trojans (ii) Viruses (iii) Worm (iv) Adware

Regulation :R13 **Code : CS427/7**

SECTION – B

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

11. Define Steganography.
12. State the types of cryptanalytic attacks.
13. Explain the security services provided by Digital Signature.
14. Point out the protocols used to provide IP security.
15. Define Logic bomb.

SECTION – C

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

16. Explain the different types of attacks.

(OR)

17. State Euler's theorem to find GCD with example.

18. Explain Secure Hashing Algorithm (SHA).

(OR)

19. Explain digital signature with Elgamal Public Key cryptosystems.

20. Illustrate PKI.

(OR)

21. Write short notes on SSL.

22. Analyse birthday attack.

(OR)

23. Outline the properties of hashing function in cryptography.

SECTION – D

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

24. Illustrate Feistel encryption and decryption.

(OR)

25. What is the need for AES? Explain its operation in detail.

26. Write about Virus and its types in detail.

(OR)

27. Demonstrate Trusted Systems.