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: CS427/6**

IV B.Tech I Semester Supplementary Examination –June, 2018

CRYPTOGRAPHY AND NETWORK SECURITY

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

SECTION – A

(Short Answer Questions)

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

1. An attempt to make a computer resource unavailable to its intended users is called
   a) denial-of-service attack b) virus attack c) Worms attack d) botnet process
2. Pretty good privacy (PGP) is used in
   a) Browser security b) email security c) FTP security d) computer security
3. DES algorithm have ……..numbers of rounds and …….bits length of key
4. Consider the scenarios.
   1) A wifi connection without encryption.
   2) Presence of malicious virus
   3) Authentication with weak password.
   In network security paradigm given scenarios can be classified as:
   a) I Threat II Threat III Vulnerability
   b) I Vulnerability II Threat III Threat
   c) I Threat II Vulnerability III Vulnerability
   d) Vulnerability 2. Threat 3. Vulnerability

5. AES has three different configurations with respect to the number of rounds and
   a) Data size b) Round size c) Key size d) Encryption size

6. A sender is employing public key cryptography to send a secret message to a receiver. Which one of the following statements is TRUE?
   a) Sender encrypts using receiver's public key
   b) Sender encrypts using his own public key
   c) Receiver decrypts using sender's public key
   d) Receiver decrypts using his own public key
7. IPsec defines two protocols: _____ and _____.
   a) AH; SSL b) PGP; ESP c) AH; ESP d) none of the above
8. SSL provides _____.
   a) message integrity b) confidentiality c) compression d) all of the above
9. Mechanism to protect private networks from outside attack is
   a) Firewall b) Antivirus c) Digital signature d) Formatting
10. RSA encryption system is
    a) Symmetric key encryption Algorithm c) Assymetric key encryption algorithm
    b) not an encryption algorithm d) None of the above

SECTION – B

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

11. Why RC4 is used in mobile system?
12. What is a message authentication code?
13. Encrypt the "VIGNAN" using *Caesar cipher.*
14. What is PGP and its main services?
15. What is Firewall and its types?

SECTION – C

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

16. Explain the S/MIME? Why it is used? Discuss the various functions of S/MIME

(OR)

17. Describe the functions and features of Kerberos.
18. Explain RSA algorithm with an example.

(OR)

19. How we achieve the integrity with help of HASH Algorithm? Which properties of hash algorithm make it robust? Is there any role of digital signature to provide the integrity in Network Security System?
20. Suppose the message KLVFAREDAAVGOOEWSTLPSYTQOBZBVBLSQMDIFIYCHVBRGQIHQGY BVWAEZCQAFIUTSNVBAE" is used as cipher text in ***transposition*** then what will be plain text where key is 2 4 3 1 5 7 9 8 6.

(OR)

21. Encryption the "**COMPUTER SCIENCE AND ENGINEERING**" where key is **DEPARTMENT** using playfair technique.
22. Explain the basic cryptographic security model.

(OR)

23. What is effect on system performance of simultaneous application of all the security services? Explain it with suitable example

SECTION – D

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

24. Write short notes on the following
    (i) Trojan Horse (ii) Worm (iii) Trapdoor (iv) Intrusion Detection (v) Zombie

(OR)

25. Discuss SSL protocol architecture. How does SET work? Describe dual signature for SET and its purpose.
26. What is the objective of AES? Explain the functioning of AES in the detail.

(OR)

27. Using S-DES, decrypt the string (10100010) using the key (0111111101). The required information is as follows ;

P8								P10										IP							
6	3	7	4	8	5	10	9	3	5	2	7	4	10	1	9	8	6	2	6	3	1	4	8	5	7

IP^{-1}								E/P								P4			
4	1	3	5	7	2	8	6	4	1	2	3	2	3	4	1	2	4	3	1

$$S0 = \begin{pmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{pmatrix}$$

$$S1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{pmatrix}$$