IV B. Tech I Semester Examination – November 2017

**CRYPTOGRAPHY AND NETWORK SECURITY**

Time: **3** hours (CSE/IT) 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. Encryption using RSA is represented as

a) C=Me mod n b) C=Md mod n c) M=Ce mod n d) None

5. The four types of active attacks are \_\_\_\_\_\_\_\_\_\_\_ .

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 \_\_\_\_\_\_\_\_\_.

1. 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. The length of plain text in DES is

a) 64 bits b) 128 bytes c) 56 bits d) None

**SECTION – B**

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

1. What are the various ways of public key distribution?
2. What is a message authentication code?
3. Encrypt the “VIGNAN” using Caesar cipher, with shift=3.
4. What is X.509 Certificate?
5. What is Firewall and its types?

**SECTION – C**

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

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

**(OR)**

1. Describe the functions and features of Kerberos.
2. Write the procedure for finding GCD and Find out the GCD (4655, 12075).

**(OR)**

1. Write RSA algorithm with example.
2. 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)**

1. Encryption the “**COMPUTER SCIENCE AND ENGINEERING**” where key is **DEPARTMENT** using playfair technique.
2. Explain the basic cryptographic network security model.

**(OR)**

1. Explain various security attacks and security services.

**SECTION – D**

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

1. Write short notes on the following

(i) Trojan Horse (ii) Worm (iii) Trapdoor (iv) Intrusion Detection (v) Zombie

**(OR)**

1. Discuss SSL protocol architecture. How does SET work?
2. What is the objective of AES? Explain the functioning of AES in the detail.

**(OR)**

1. 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 |