(Pages : 2) **D – 3551**

Reg. No. : .....

Name : .....

Eighth Semester B.Tech. Degree Examination, December 2017
(2008 Scheme)
08.803 : CRYPTOGRAPHY AND NETWORKS SECURITY (R)

Time : 3 Hours Max. Marks : 100

PART – A

Answer **all** questions.

1. Distinguish between a substitution cipher and a transposition cipher.
2. Mention the attacks on AES.
3. Why does the DES function need an expansion permutation ?
4. What is S-box ? Mention the necessary conditions for an S-box to be invertible.
5. What are the principal elements of a public key cryptosystem ?
6. Write the verification process of Digital Signature Algorithm (DSA).
7. If the length of the message is 6143 bits, how many padding bits are needed in Secure Hash Algorithm (SHA) ?
8. In Pretty Good Privacy (PGP) explain how users A and B exchange the secret key for encrypting messages.
9. List the services provided by IPSec.
10. Write notes on SET (Secure Electronic Transaction). **(10×4=40 Marks)**

PART – B

Answer **one full** question from **each** Module.

Module – I

11. a) Draw the general structure of AES and explain the encryption decryption process. **12**

    b) Describe block cipher modes of operation in detail. **8**

OR

12. Encrypt the plaintext 11000110 with the key 0101010110 using S-DES algorithm.

S0 = 1 0 3 2 S1 = 0 1 2 3
3 2 1 0 2 0 1 3
0 2 1 3 3 0 1 0
3 1 3 2 2 1 0 3

E/P = {4, 1, 2, 3, 2, 3, 4, 1}

P4 = {2, 4, 3, 1}

P10 = {3, 5, 2, 7, 4, 10, 1, 9, 8, 6}

P8 = {6, 3, 7, 4, 8, 5, 10, 9}

IP = {2, 6, 3, 1, 4, 8, 5, 7}. **20**

Module – II

13. a) With the prime numbers p = 7 and q = 11, public key e = 17 and plain text M = 8, perform encryption and decryption using RSA algorithm. Explain why one could not easily break the cipher text by knowing the cipher text and the value of the prime numbers. Describe the trapdoor behind this RSA cryptosystem. **12**

b) How are secret keys distributed by making use of public key cryptography ? **8**

OR

14. Users A and B use the Diffie Hellman protocol for key exchange with a common prime q = 37 and a primitive root 13. Users private key are $X_A = 10$ and $X_B = 7$.

a) Find the public keys. **7**

b) What is the value of the symmetric key ? **7**

c) What happens if an adversary takes over the public key sent by A ? **6**

Module – III

15. a) Explain the firewall configurations in detail. **10**

b) Draw the SSL protocol stack and explain its components. **10**

OR

16. a) Bring out the importance of security associations in IP. **10**

b) Why does PGP generate a signature before applying compression ? Explain the modules. **10**

(3×20=60 Marks)