(Pages : 2) **D – 4171**

Reg. No. : .....

Name : .....

Eighth Semester B.Tech. Degree Examination, January 2018
(2013 Scheme)
13.801 : CRYPTOGRAPHY AND NETWORK SECURITY (R)

Time : 3 Hours Max. Marks : 100

PART – A

Answer **all** questions : **(5×4=20 Marks)**

1. Which security mechanism(s) are provided in each of the following cases ? Justify.
   i) A College demands student id and password to let students log into the College Intranet.
   ii) A Bank Server disconnects a customer if he/she is logged into the system for more than one hour.
   iii) A Bank requires a customer signature for a withdrawal.
2. Explain the block cipher operation modes that can be sped up by parallel processing.
3. If the length of the message is 6143 bits, how many padding bits are needed in Secure Hash Algorithm (SHA) ?
4. In Pretty Good Privacy (PGP) explain how users A and B exchange the secret key for encrypting messages.
5. Mention the services provided by SSL Record Protocol.

PART – B

Answer **one full** question from **each** Module. **(4×20=80 Marks)**

MODULE – I

6. a) Show how Feistel network is used in DES Algorithm. Also explain the Encryption and Decryption process. **10**
   b) Explain the avalanche effect of DES. **10**

OR

7. a) Describe the block cipher modes of operation in detail. **10**
   b) Draw the basic structure of AES and explain its components. **10**

P.T.O.

MODULE – II

8. Users A and B use the Diffie Hellman protocol for key exchange with a common prime q = 23 and a primitive root 7. Users private key are $X_A = 3$ and $X_B = 5$.
   i) Find the public keys. **5**
   ii) What is the value of the symmetric key ? **5**
   iii) Write the algorithm. **10**

OR

9. Describe the process of encryption and decryption using Elliptic Curves. Consider the Cryptosystem parameters $E_{67}(2, 3)$ and G(2, 22). B's Secret key is $n_B = 2$. A wishes to encrypt the message $P_m = (24, 26)$ and chooses the random value k = 2. Determine the cipher text C_m. Show the calculation by which B recovers P_m from C_m. **20**

MODULE – III

10. a) Give the general format of PGP message. **5**
    b) Explain S/MIME IP Security in detail. **15**

OR

11. What are public key certificates ? Why are they important ? Illustrate with an example. **20**

MODULE – IV

12. a) Explain the types of firewalls in detail. **15**
    b) Briefly explain the purpose of SSL alert protocols. **5**

OR

13. Explain Secure Electronic Transaction (SET) in detail. **20**
