(Pages : 3)



**E – 5581**

Reg. No. : .....

Name : .....

# Eighth Semester B.Tech. Degree Examination, October 2018
## (2008 Scheme)
## 08.803 : CRYPTOGRAPHY AND NETWORKS SECURITY (R)

Time : 3 Hours  Max. Marks : 100

PART – A

Answer **all** questions. **Each** question carries **4** marks.

1. How block size, key size and number of rounds of a Feistel Network relates to its security ?
2. What is the difference between block and stream cipher ? Give one example for each.
3. How mono-alphabetic cipher is vulnerable to frequency attack ?
4. Draw a block diagram showing how hash function and encryption technique can be used as digital signature.
5. What is the zero point in elliptic curve ?
6. Define weak collision resistance and strong collision resistance.
7. Write any two benefits of providing security at IP level (IP Sec.)
8. How SSL connection is different from SSL session ?
9. What is the purpose of the state array ?
10. What requirements should a digital signature scheme satisfy ? **(10×4=40 Marks)**

**P.T.O.**

PART – B

Answer **one full** question from **each** Module. **Each** question carries **20** marks.

**Module – I**

11. a) Describe the key expansion algorithm of AES. **10**

    b) Describe linear cryptanalysis of DES. **10**

OR

12. a) Explain single round operation of DES algorithm. **10**

    b) What are the basic operations in IDEA ? Explain with diagram, the sequence of operations in IDEA. **10**

**Module – II**

13. a) In Diffie-Hellman protocol, primitive root $\alpha = 7$, common prime $q = 23$, $x = 3$ and $y = 5$ are secret numbers selected by Alice and Bob. What is the value of secret key exchanged between them ? **10**

    b) Explain the concept behind Elliptic curve cryptography. Write steps for key exchange using ECC. **10**

OR

14. a) Write RSA algorithm. Perform encryption and decryption using the RSA algorithm for

    $p = 5$; $q = 11$; $e = 3$; $M = 9$. **8**

    b) Describe single step operation of SHA1. **12**

## Module – III

15. a) Explain the functions provided by S/MIME. **6**

b) What is the differences between Transport and Tunnel mode operation ? **6**

c) Draw structure of IPv4AH packets in transport mode and tunnel mode operation. **8**

OR

16. a) What is the difference between a packet filtering router and a stateful inspection firewall ? **10**

b) Explain with a block diagram how confidentiality and authenticity be provided using PGP. **10**