



Reg. No. :

Name :

Eighth Semester B.Tech. Degree Examination, April 2015
08.803 : CRYPTOGRAPHY AND NETWORK SECURITY (R)

Duration : 3 Hours

Total Marks : 100

PART – A

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

- I. 1) List the parameters (block size, key size and number of rounds) for three AES version.
- 2) Use extended Euclidean algorithm to find multiplicative inverse of 9 in Z_{26} .
- 3) Use Vignere cipher with keyword 'HEALTH' to encipher the message 'full of surprises'.
- 4) Define a Security Association.
- 5) Draw possible scheme for authentication using a public key encryption system.
- 6) Define weak collision resistance and strong collision resistance.
- 7) Write any two benefits of providing security at IP level (IP Sec).
- 8) What is the function of Handshake protocol in SSL ?
- 9) Show how public keys can be distributed using public key certificates.
- 10) What is steganography ?

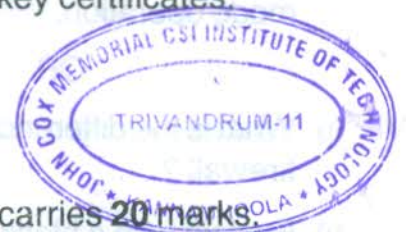
PART – B

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

Module – I

- | | |
|--|-----------|
| II. a) Describe Mixcolumn transformation of AES. | 8 |
| b) Discuss how DES can be used to encrypt/decrypt blocks of size less than 64. | 12 |

OR





- III. a) For each of the following ciphers, say whether it is stream cipher or block cipher. Defend your answer.
- i) Play Fair
 - ii) Auto key
 - iii) One time pad
 - iv) Rotor Machines. 8
- b) Explain single round operation DES algorithm. 12

Module – II

- IV. a) Write Digital Signature Algorithm. 10
- b) Explain how a common key is established between communicating parties using Diffie-Hellman Algorithm. 10
- OR
- V. a) Describe single step operation of MD5. 10
- b) Explain the concept behind Elliptic curve cryptography. Write steps for key exchange using ECC. 10

Module – III

- VI. a) Explain the functions provided by S/MIME. 8
- b) What is the differences between Transport and Tunnel mode operation ? 4
- c) Draw structure of IP v4 AH and ESP packets in transport mode and tunnel mode operation. 8
- OR
- VII. 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