Code: 13A05702 **R13**

B.Tech IV Year I Semester (R13) Regular Examinations November/December 2016

CRYPTOGRAPHY & NETWORK SECURITY

(Computer Science and Engineering)

Time: 3 hours Max. Marks: 70

PART – A

(Compulsory Question)

*****

1 Answer the following: (10 X 02 = 20 Marks)

(a) What is Steganography?

(b) Explain about Security Attacks.

(c) What are the three properties of Modular Arithmetic?

(d) Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 11 and a primitive root α = 2. If user A has private key X_A = 5, what is A's public key Y_A?

(e) Give the requirements for a Hash Function.

(f) Define MAC (Message Authentication Code).

(g) List out the headers of S/MIME.

(h) Explain about Distribution of public keys.

(i) Explain about Security Association Parameters.

(j) Explain the Intrusion detection tool audit records.

PART – B

(Answer all five units, 5 X 10 = 50 Marks)

UNIT – I

2 Explain different block cipher modes of operation..

OR

3 Explain security mechanisms in detail.

UNIT – II

4 Explain the procedure involved in RSA public-key encryption algorithm.

OR

5 Explain about the Chinese Remainder theorem.

UNIT – III

6 With an example, explain about SHA-1 algorithm.

OR

7 Explain briefly about Digital Signature Standard.

UNIT – IV

8 Explain what Kerberos is and give its requirements.

OR

9 Explain the X.509 authentication procedures.

UNIT – V

10 What are the steps involved in the SSL record protocol transmission?

OR

11 (a) Explain the principles and limitations of a firewall.

(b) Describe the main characteristics of computer virus.

*****