Code: 13A05702 **R13**

B.Tech IV Year I Semester (R13) Supplementary Examinations June 2017

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) Find the plaintext for the given Cipher text with Key K = 3.
Using Ceaser Cipher. Cipher Text : GUDSMDEGXONDODP

(b) Define Avalanche Effect.

(c) Determine the Numbers which are Relatively Prime to 21 by using Euler Totient Function.

(d) Differentiate conventional and public key encryption.

(e) Give the requirements for a Hash Function.

(f) Define MAC (Message Authentication Code).

(g) Differentiate forward and reverse certificates.

(h) What is S/MIME?

(i) Sketch neatly the SSL protocol stack.

(j) What are the benefits of IPSec?

PART – B

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

UNIT – I

2 Write short notes on security mechanisms.
Explain in detail about the steps involved in DES.

OR

3 Explain in detail about AES.
Give an account on different block cipher modes of operation.

UNIT – II

4 Perform Encryption and Decryption using the RSA algorithm.
p = 3 q = 11 e = 7 M = 5

OR

5 Explain in detail about Elgamal Cryptosystem and Chinese Remainder theorem.

UNIT – III

6 With an example, explain in detail about Secure Hash Algorithm.

OR

7 Explain in detail about HMAC and Digital Signature Standard..

UNIT – IV

8 Sketch neatly and briefly explain about Public Key Infrastructure.

OR

9 Explain in detail about Kerberos.

UNIT – V

10 Explain in detail about SSH and SSL record protocol transmission.

OR

11 Explain in detail about IP Security Policy.

*****