Code: 13A12602 **R13**

B.Tech III Year II Semester (R13) Supplementary Examinations December 2016

CRYPTOGRAPHY & NETWORK SECURITY

(Information Technology)

Time: 3 hours Max. Marks: 70

PART – A

(Compulsory Question)

*****

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

(a) Define Masquerade Attack.

(b) Construct the Keyword matrix for “SPECULATE” using play fair Cipher.

(c) Give the algorithm for primality testing using Miller Rabin algorithm.

(d) Define trap-door one-way function.

(e) What are Cryptographic Hash Functions?

(f) Give the diagram of CMAC encryption.

(g) How can we use Asymmetric Encryption to establish a Session key? Give diagram.

(h) List the examples for replay attacks.

(i) Give the Protocol Stack of SSL Architecture.

(j) List the elements of HTTPS.

PART – B

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

UNIT – I

2 Consider the plain text “Paymoremoney” and use the following matrix as encryption key. Show the steps for encryption of the plaintext using Hill Cipher. Give the decryption key of the key matrix.

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

OR

3 Explain with a neat diagram, working of Single Round of Data Encryption Standard (DES) Block cipher algorithm.

UNIT – II

4 Explain with an example, the Discrete Logarithms of a given number.

OR

5 Given plaintext M = 10, p = 7, q = 13 and e = 5. Perform RSA Encryption and Decryption process.

UNIT – III

6 Explain the structure of HMAC Algorithm with a neat diagram.

OR

7 Compare the RSA and DSS approaches for generation of Digital Signature with suitable diagrams.

UNIT – IV

8 Explain with a neat diagram, the concept of Public key distribution of Secret keys.

OR

9 Explain the simple Authentication Dialogue of Kerberos for authentication service.

UNIT – V

10 Describe the importance of HTTPS protocol along with Connection Initiation and Connection Closure.

OR

11 Explain the following two modes of IPSec services:

(a) Transport Mode.

(b) Tunnel Mode.

*****