Code: 13A12602 **R13**

B.Tech III Year II Semester (R13) Regular Examinations May/June 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) List and define the two related concepts covered by the term “Integrity”.

(b) Encrypt the following message using Caesar Cipher: meet me after the toga party.

(c) Find the greatest common divisor of 2740 and 1760 using Euclidean algorithm.

(d) Define Group and Commutative Group.

(e) Define the following properties related to cryptographic hash functions:
(i) One-way property. (ii) Collision-free prope.

(f) Write the requirements for digital signatures.

(g) What is the difference between a session key and a master key?

(h) List the requirements of Kerberos.

(i) Mention the SSL session state parameters.

(j) What are the advantages of Packet Filters?

PART – B

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

UNIT – I

2 (a) Draw the Symmetric Cipher model. What are the two requirements for secure use of symmetric encryption?

(b) Based on choice of what parameters and design features,the exact realization of a Feistel network depends. Explain.

OR

3 With neat diagrams, describe the block cipher modes of operations and give typical applications of each.

UNIT – II

4 (a) Write the Miller-Robin test algorithm.

(b) Explain why RSA works.

OR

5 Explain Diffie-Hellman Key Exchange and give an example.

UNIT – III

6 (a) What types of attacks are addressed by message authentication? Explain in detail.

(b) Illustrates the overall operation of HMAC and explain.

OR

7 (a) List and explain the threats associated with a direct digital signature scheme.

(b) With a neat diagram explain the Digital Signature Model.

UNIT – IV

8 Draw the formats of X.509 certificate and certificate revocation list and explain each field of the certificate.

OR

9 (a) Why does PGP generate a signature before applying compression?

(b) Give the format of PGP public key ring and explain each field.

UNIT – V

10 Explain the two protocols defined by IPSec.

OR

11 Write short notes on the following:

(a) Buffer overflows

(b) Worms

(c) Virus

*****