Code: 9D08205

M.Tech II Semester Supplementary Examinations February 2018

CRYPTOGRAPHY & NETWORK SECURITY

(Computer Networks)

(For students admitted in 2012, 2013, 2014, 2015 & 2016 only)

Time: 3 hours Max. Marks: 60

Answer any FIVE questions

All questions carry equal marks

*****

1 (a) What is an attack? List the types of attacks. Briefly describe the classification of attacks.
(b) Define various mathematical tools for cryptography in details.

2 Explain the process of encryption and decryption in DES (Data encryption standard) algorithm.

3 (a) Illustrate with an example the process involved in RSA algorithm.
(b) Define digital signature. Explain its role in network security.

4 (a) Define and explain various user authentication protocols.
(b) Give the complete clarity among HMAC and CMAC.

5 (a) Explain the digital signature algorithm with an example.
(b) What is public key infrastructure? How PKI is managed in India?

6 Explain security handshake pitfalls in detail.

7 (a) Explain the operational description of (pretty good privacy) PGP.
(b) Explain X.509 authentication service.

8 (a) Explain the intrusion detection tool audit records.
(b) List and briefly define four techniques used to avoid guessable password.

*****