Code: 9D08205

M.Tech II Semester Supplementary Examinations January/February 2017

CRYPTOGRAPHY & NETWORK SECURITY

(Computer Networks)

Time: 3 hours Max. Marks: 60

Answer any FIVE questions
All questions carry equal marks

*****

1 (a) Differentiate between:
(i) Substitution and transportation ciphers.
(ii) Symmetric and Asymmetric key cryptography.
(iii) Passive and active attacks.
(iv) Cryptography and steganography.
(b) Distinguish among vulnerability, threat and control.

2 (a) Explain the round function used in DES with a neat diagram.
(b) What primitive operations are used in RC4? Explain.

3 (a) Give a brief note on attacks on RSA.
(b) Explain the threats associated with a direct digital signature scheme.

4 (a) What are the HMAC design objectives as per the RFC's?
(b) With the help of neat diagrams, explain the varieties of ways in which a hash code is used to provide message authentication. How does a hash function differ from MAC?

5 (a) What are the core components of a PKI? Briefly describe each component.
(b) Give a brief note on PKCS.

6 (a) What do you mean by singe sign on approach? Mention its advantages.
(b) Make comparisons between the certified based authentication and biometric authentication.

7 (a) How an SSL session is established using SSL Handshake protocol?
(b) List and explain the applications of IPSec.

8 (a) Discuss about Markov model for the generation of guessable passwords.
(b) What is a virus? How it is different from a worm? List some of the latest virus that you have listened about and describe how it has propagated.

*****