Code: 9D06106a

M.Tech II Semester Supplementary Examinations January/February 2017

NETWORK SECURITY & CRYPTOGRAPHY

(Electronics & Communication Engineering)

Time: 3 hours Max. Marks: 60

Answer any FIVE questions

All questions carry equal marks

*****

1 (a) What are the various services to be offered for enhancing the security of the information processing system?
(b) Explain the different security attacks in detail.

2 (a) Explain a symmetric encryption scheme and its ingredients.
(b) Explain the block cipher which is a Feistel structure that makes use of key dependent S-boxes.

3 (a) State and prove Fermat's and Euler's theorem.
(b) Explain Diffie – Hellman key exchange algorithm.

4 (a) Explain how message authentication is achieved.
(b) What is Hash function? Explain some approaches for producing message authentication.

5 (a) Explain the functioning of HMAC algorithm.
(b) What is the difference between Hash and MAC functions?

6 (a) Discuss the concepts of trusted systems.
(b) Explain how X-509 authentication service works for two way authentication.

7 (a) Explain the IP security architecture in detail.
(b) What are the three threats associated with user authentication over a network or internet and explain the same.

8 (a) List and briefly explain three classes of intruders.
(b) Explain how authentication header guards against the replay attack.

*****