Code: 9D06106a

M.Tech II Semester Supplementary Examinations February 2018

NETWORK SECURITY & CRYPTOGRAPHY

(Electronics & Communication Engineering)

(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) Discuss a model for network security. Explain the broad categories of security mechanisms needed to cope with unwanted access.
(b) Explain about the following terms: (i) Security service. (ii) Steganography.

2 (a) Describe theory of block cipher design.
(b) Discuss about key generation, verification and updating.
(c) What is RC5? Explain four modes of operation in it.

3 (a) In a RSA system, the public key of a given user e = 31, n = 3599. What is the private key of this user?
(b) What are the roles of the public and private key?
(c) Illustrate Diffie-Hellman key exchange scheme for GF(P).

4 (a) Using Fermat's theorem, find 3^{201} mod 11.
(b) Explain in detail about extended Euclid's algorithm.
(c) What is the difference between message authentication code and one-way hash function?

5 (a) Explain about RIPEMD – 160 signature scheme. What are the possible attacks against this scheme?
(b) Discuss about: (i) Authentication protocols. (ii) Digital signature standards.

6 (a) What is Kerberos? What is the problem addressed by it? State the requirements for Kerberos.
(b) Outline the methods adopted for Pretty Good Privacy (PGP). Explain the digital signature services provided by PGP.

7 (a) Discuss the pay load key management issues.
(b) Explain in detail the secure socket layer protocol stack.

8 (a) Discuss the stages of a network intrusion.
(b) What are two common techniques used to protect a password file?

*****