H.T.No. | | | | | | | | | | |

Code No: CS1914 **GEC-R14**

M. Tech II Semester Regular/Suppl. Examinations, July 2017

CRYPTOGRAPHY AND NETWORK SECURITY

(Computer Science Engineering)

Time: 3 Hours **Max. Marks: 60**

Note: Answer any **FIVE** questions. All Questions carry equal Marks.

5 × 12 = 60M

1. a) Explain about pervasive security mechanisms. (5M)

   b) Explain any two non cryptographic protocol vulnerabilities. (7M)

2. a) Mention the HMAC design Objectives and discuss the security of HMAC. (6M)

   b) Explain the process of AES evaluation in detail. (6M)

3. a) Perform Encryption and decryption using RSA Algorithm for the values M=2, p=17 & q=31. (6M)

   b) Explain about the mathematical attacks on RSA. (6M)

4. a) Briefly discuss about Kerberos version 4 Authentication dialogue. (8M)

   b) What is Kerberos Realm? Explain. (4M)

5. a) Write a short note on IP Security Architecture. (8M)

   b) Explain about ESP format. (4M)

6. a) Briefly discuss about SSL Record protocol. (6M)

   b) Explain about different types and phases of Viruses. (6M)

7. Briefly discuss about SNMP. (12M)

8. a) Explain about strength of DES. (4M)

   b) Explain approaches for intrusion detection system. (8M)

*****