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

Code No: CS1522 **GEC-R14**

IV B. Tech I Semester Supplementary Examinations, February 2018

INFORMATION SECURITY

(Computer Science and Engineering)

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

Note: All Questions from **PART-A** are to be answered at one place.
Answer any **FOUR** questions from **PART-B.** All Questions Carry Equal Marks.

PART-A

6 × 2 = 12M

1. Define integrity and non repudiation.
2. List out the strengths of DES.
3. List any three public key cryptographic algorithms.
4. List the services provided by PGP.
5. SSL session state defined by what parameters?
6. List various categories of viruses.

PART-B

4 × 12 = 48M

1. Examine various software vulnerabilities. (12M)
2. a) Write a short note on Security of Hash Functions and MAC? (4M)
   b) Explain single round function of DES. (8M)
3. a) Discuss various principles of public key cryptosystems. (6M)
   b) Define Man in the middle attack. In which protocol this problem will raise? Explain. (6M)
4. a) What is replay attack? Which scheme is used to avoid replay attack show its procedure. (6M)
   b) Why does ESP include a padding field? Discuss. (6M)
5. a) What is alert protocol? Discuss various alerts used in SSL protocol. (6M)
   b) Briefly describe key features of SET and SET participants. (6M)
6. a) What are the various classes of Intruders? List and explain various techniques used by intruders for learning passwords. (6M)
   b) Explain UNIX password scheme. What are the possible threats to it? (6M)

*****