No. of Printed Pages : 2     **BICSE-016**

# B.Tech. - VIEP - COMPUTER SCIENCE AND ENGINEERING

## (BTCSVI)

# Term-End Examination, 2019

## BICSE-016 : CRYPTOGRAPHY AND NETWORK SECURITY

**Time : 3 Hours]**     **[Maximum Marks : 70**

**Note :** Attempt **any five** questions in all. Each question carries equal marks.

1. (a) What is cipher ? Differentiate between substitution cipher and transposition cipher. [7]

   (b) What is key exchange algorithm ? Explain. [7]

2. (a) What is the different types of attacks on double DES and Triple DES ? [7]

   (b) Discuss the use of authentication protocols ?[7]

3. (a) Explain the RSA crypto system. Also explain how decryption be made fast. [7]

   (b) Discuss secret key cryptography. [7]

BICSE-016     ( 1 )     [P.T.O.]

4. (a) Discuss in detail about Diffie-Hellman key exchange algorithm with the help of an example. [7]

   (b) What is meant by Block Cipher ? [7]

5. Describe the security issues and security factors in wireless LAN Network. [14]

6. Explain key generation, encryption and decryption in the RSA algorithm. [14]

7. Write short notes on the following : [4x3.5=14]

   (a) Intrusion Detection

   (b) Trojan Horse

   (c) Kerberos

   (d) Socket

----- x -----