BICSE-016

B.Tech. – VIEP – COMPUTER SCIENCE AND ENGINEERING (BTCSVI)

Term-End Examination

00283

June, 2018

BICSE-016 : CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 hours *Maximum Marks : 70*

Note : *Answer any* **five** *questions. All questions carry equal marks.*

1. Explain the concept of Feistel encryption and Decryption algorithm. *14*

2. (a) What is the difference between active and passive security threats ? *7*

   (b) List and briefly define categories of security devices. *7*

3. What is meant by message authentication ? Explain about the functions of authentication in detail. *14*

4. Describe in detail the concept of pretty good privacy along with its application. *14*

5. What is a firewall ? How is it useful ? Explain the firewall design principle in detail. *14*

6. Explain RSA algorithm with an example. List the possible attacks on it. *14*

7. (a) What problem was Kerberos designed to address ? *7*

(b) What four requirements were defined for Kerberos ? *7*

_____