00358

No. of Printed Pages : 2

BICSE-016

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

Term-End Examination

December, 2015

BICSE-016 : CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 hours *Maximum Marks : 70*

Note : *Attempt any **seven** questions. Each question carries equal marks.*

1. Explain the various security services and mechanisms in detail. *10*

2. What were the classical encryption techniques ? Explain the various substitution ciphers in detail using suitable examples. *10*

3. Explain the modern Block Ciphers in detail along with the Block Cipher principles. *10*

4. What is DES ? Using a suitable diagram, explain its one complete iteration in detail. *10*

5. Differentiate between public key cryptography and private key cryptography techniques in detail. Also explain the concept of elliptical curve cryptography technique. *10*

6. Describe the RSA algorithm in detail. Also illustrate the RSA algorithm with p = 3 and q = 5. *10*

7. Explain the following terms with the help of examples : *10*

   (a) Message Authentication Code

   (b) Hash Function

   (c) Birthday Attacks

8. Explain the MD5 message digest algorithm in detail. *10*

9. Describe in detail the concept of pretty good privacy along with its applications. *10*

10. What is a Firewall ? How is it useful ? Explain the firewall design principle in detail. *10*
