No. of Printed Pages : 2

BICSE-016

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

Term-End Examination

00746

June, 2016

BICSE-016 : CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 hours *Maximum Marks : 70*

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

1. Explain the concept of Feistel Encryption and Decryption algorithms. *14*

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

3. Explain key generation, encryption and decryption in the RSA algorithm. *14*

4. How is double DES achieved ? Under what condition is the above reduced to single encryption ? *14*

5. What is the difficulty posed to an opponent when Diffie-Hellman key exchange algorithm is used in public key cryptography ? Show necessary steps in support of your answer. *14*

6. How does symmetric key cryptography and asymmetric key cryptography get used in digital signatures ? *14*

7. (a) Describe about SHA algorithm and compare its features with MD5. *7*

   (b) Discuss in detail about Diffie-Hellman key exchange algorithm with the help of an example. *7*