No. of Printed Pages : 2

BICSE-016

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

Term-End Examination

December, 2016

00903

BICSE-016 : CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 hours *Maximum Marks : 70*

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

1. Explain how the man-in-the-middle attack can be done on Diffie-Hellman key exchange algorithm. What features are added in the Oakley protocol to counter this attack ? *14*

2. Explain a single round of DES algorithm with the help of a neat diagram. *14*

3. Explain RSA algorithm with an example and test for primality. Also list the possible attacks on it. *14*

4. (a) What are the two different uses of public key cryptography related to key distribution ? *7*

   (b) Discuss Diffie-Hellman key exchange algorithm. *7*

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

6. (a) What is meant by Block Cipher ? *7*

   (b) What are the key algorithms used in S/MIME ? *7*

7. Give any two parameters and design choices that determine the actual algorithm of a Feistel Cipher. *14*
