No. of Printed Pages : 2

BICSE-016

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

Term-End Examination

June, 2015

00129

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 term Cryptography. Also explain the various security attacks and their types. *10*

2. State and describe the conventional encryption model. Also differentiate between Cryptanalysis and Steganography in detail. *10*

3. What is the Shannon's theory of Confusion and Diffusion ? Also explain the Fiestel structure in detail. *10*

4. Explain in detail the IDEA encryption and decryption algorithm along with the description of its strength. *10*

5. What is the Fermat's and Euler's theorem ? Explain using suitable examples. Also describe Primality Testing in detail. *10*

6. Using a suitable example, explain the Diffie-Hellman key exchange algorithm. *10*

7. Explain the usefulness of discrete logarithms concept in terms of security. Also explain the ElGamal encryption technique in detail. *10*

8. What are Digital Signatures ? Propose the proof of the digital signature algorithm. *10*

9. Explain the directory authentication service in detail. *10*

10. Explain the architecture of IPsec along with the decryption of its authentication header. Also explain the concept of secure electronic transaction. *10*