No. of Printed Pages : 2

BICSE-016

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

00336

Term-End Examination

December, 2014

BICSE-016 : CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 hours *Maximum Marks : 70*

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

1. (a) List and briefly define the categories of passive and active security attacks. *5*

(b) What are the two general approaches to attack a cipher ? *5*

2. Explain the concept of Feistel Encryption and Decryption algorithms. *10*

3. (a) What type of information can be derived from a traffic analysis attack ? *5*

(b) What is cryptographically generated Random number ? Explain with examples. *5*

4. (a) State the procedure for determining the greatest common divisor of two positive integers. Explain with examples. *5*

(b) Explain Fermat's and Euler's theorems respectively. *5*

5. (a) What are three broad categories of applications of public key crypto systems ? *5*

(b) State and explain RSA algorithm. *5*

6. (a) What are some approaches to producing message authentication ? *5*

(b) What is the difference between a message authentication code and a one-way hash function ? *5*

7. (a) What is the difference between little-endian and big-endian format ? *5*

(b) What basic arithmetical and logical functions are used in SHA ? *5*

8. (a) What is the purpose of X.509 Standard ? *5*

(b) When is an X.509 Certificate revoked ? *5*

9. (a) What are the five principal services provided by PGP ? *5*

(b) Why does PGP generate a signature before applying compression ? *5*

10. (a) What is the difference between SSL connection and SSL session ? *5*

(b) How many steps are involved in the SSL record protocol transmission ? *5*
