B.TECH. COMPUTER SCIENCE AND ENGINEERING (BTCSVI)

Term-End Examination

June, 2013

BICSE-016 : CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 hours *Maximum Marks : 70*

Note : *(i)* *Answer **any seven** questions.*

(ii) *All questions **carry equal** marks.*

1. (a) What is the difference between strong collision and weak collision resistance ? 5

   (b) What is the role of a compression function in a hash function ? 5

2. (a) What are the fields present in SSL record protocol header ? Mention their purpose and size. 5

   (b) Discuss the purpose of change cipher spec protocol and alert protocol in detail. 5

3. (a) Explain the process of Encryption and Decryption in Elliptic curve cryptography. 5

   (b) Compare RSA with PCC. 5

4. (a) What is R64 conversion ? Why is R64 conversion useful for an e-mail application ? 5

(b) Why is the segmentation and reassembly function in PGP needed ? 5

5. (a) What is hash function ? List the requirement for a hash function. 5

(b) Explain the Digital Signature Standard (DSS) algorithm. 5

6. (a) What are the requirement for public - key cryptography ? Also enumerate some applications of public key crypto systems. 5

(b) Explain the motivations for Kerberos application. Also list the requirements for the same. 5

7. What is meant by message authentication ? Explain about the functions of authentication in detail. 10

8. (a) Explain about the block cipher modes of operation in detail. 5

(b) What is the importance to study the Feistel Cipher structure ? 5

9. Explain how man - in - the middle attack can be done on Diffie - Hellman algorithm. What features are added in Oakley protocol to counter this attack ? **10**

10. Write short notes on :

(a) Trapdoor **2½**

(b) Logic bomb **2½**

(c) Virus **2½**

(d) Trojan Horse **2½**