No. of Printed Pages : 2

BICSE-016

00561

B.TECH. COMPUTER SCIENCE AND ENGINEERING (BTCSVI)

Term-End Examination

December, 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. Write short notes on :

(a) Random Number generation. 5

(b) Public key cryptography. 5

2. (a) State and prove Fermat's Theorem. 5

(b) State and prove Euler's theorem. 5

3. (a) Explain the general format of a PGP message with a pictorial representation. 5

(b) What is a certification authority and explain its role in S/MIME. 5

4. What protocol is used to convey SSL related alerts to the peer entity ? Give the format of protocol. Describe the fields. 10

5. (a) Explain about the principals of public key crypto systems in detail. 5

(b) Discuss about the Elganel encryption. 5

6. What is meant by authentication? Explain the usage of Kerveros in a distributed environment. 10

7. (a) Discuss the Shanon's theory of confusion and diffusion. 5

   (b) Write about Chonese Remainder Theorem. 5

8. (a) With a suitable example show how digital signature provides security. Also highlight the advantages of Digital Signature. 5

   (b) Explain the terms used in relation with x.509 certificate. 5

   (i) version

   (ii) Serial number

   (iii) Issuer unique identifier

   (iv) Signature algorithm identifier

   (v) Subject unique identifier.

9. (a) Discuss in detail about any two proxy based firewalls. 5

   (b) Discuss the basic concept of data access control. 5

10. (a) Explain how stream cipher is different from the one-time pad. 5

    (b) Compare the different versions of Secure Hash Algorithm (SHA) that were released. 5