No. of Printed Pages : 2

BICSE-016

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

00604

Term-End Examination
June, 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) What is the difference between passive and active security threats ? *5*

   (b) List and briefly define categories of security services. *5*

2. Explain the single round of DES Algorithm with neat diagram. *10*

3. (a) List important design considerations for a Stream cipher. *5*

   (b) What primitive operations are used in RC4 ? *5*

4. (a) Define Modular arithmetic. What are the operations in modular arithmetic ? *5*

(b) What is Chinese remainder theorem ? Explain the assertions in CRT. 5

5. (a) What are the differences between conventional and public-key encryption ? 5

(b) What are the two different uses of Public-Key Cryptography related to key distribution ? 5

6. (a) What types of attacks are addressed by message authentication ? 5

(b) What two levels of functionality comprise a message authentication or digital signature mechanism ? 5

7. (a) What are the properties a digital signature should have ? 5

(b) Explain the two approaches to digital signature standards. 5

8. (a) What problem was Kerberos designed to address ? 5

(b) What four requirements were defined for Kerberos ? 5

9. (a) What are the five header fields defined in MIME ? 5

(b) What are the functions in S/MIME functionality ? 5

10. (a) Give examples and applications of IPsec. 5

(b) What services are provided by IPsec ? 5