IT 8 – 2 (RC)

B.E. (IT) (Semester – VIII) Examination, June 2013
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY
(Revised Course)

Duration : 3 Hours | Total Marks : 100

Instructions : *1) Attempt **any five** questions selecting atleast **one** question from **each** Module.*
*2) Figures to the **right** indicate **full** marks.*

Module – I

1. a) Write a note on Substitution and Transposition encryption techniques. **6**
   b) Explain the following w.r.t. encryption scheme :
      i) Unconditionally secure
      ii) Computationally secure. **4**
   c) Distinguish between active and passive attack. **4**
   d) Explain the digital immune system with the help of figure. **6**

2. a) Describe the model for network security that is needed for 2 principals to securely exchange message. **5**
   b) How does columnar transposition work ? Illustrate Encryption and Decryption operation with an example. **6**
   c) Explain the approaches to Intrusion detection. **4**
   d) Explain the compression virus with a neat diagram. **5**

Module – II

3. a) What are the potential locations for Confidentiality attacks ? **4**
   b) Explain the CTR mode of operation of DES with its advantages. **7**
   c) What is the purpose of S-box ? How does it work ? **3**
   d) Explain a Transparent Key Control Scheme. **6**

4. a) Explain how control vector scheme is used for Controlling Key Usage. **7**
   b) State Fermat's and Euler's theorems. **3**
   c) Explain CBC mode of operation of DES. **4**
   d) Compare Link Encryption and End-to-End Encryption. **6**

P.T.O.

Module – III

5. a) Explain the following techniques for distribution of public keys : 7
   i) Public Key Authority
   ii) Public Key Certificates.

   b) Consider the following parameters for Diffie-Hellman Key Exchange : $q = 97$, $\alpha = 5$, Secret keys $Xa = 36$, $Xb = 58$. Compute the public keys Ya, Yb and the common secret key K. 6

   c) Explain MD5 message digest algorithm with the help of diagram. 7

6. a) Perform encryption and decryption using RSA algorithm for $p = 7$, $q = 13$ and $e = 5$ for Message = 10. 7

   b) Describe the Arbitrated Digital Signature. 6

   c) What are the requirements for a Hash Function ? Explain one basic use of Hash Functions. 5

   d) Which are the 3 classes of functions used to produce Authenticator ? 2

Module – IV

7. a) Explain the messages exchanged by Client C, Authentication Server (AS) and Ticket Granting Service (TGS) in Kerberos. What is the overall purpose of these messages ? 7

   b) Describe the participants of SET with a neat diagram. 7

   c) What is a dual signature ? State its purpose and explain its construction. 6

8. a) Explain the following services of PGP : 6
   i) Compression
   ii) Segmentation and Reassembly.

   b) What are the functions of S/MIME ? 4

   c) Write a note on Firewall Configurations. 7

   d) Differentiate between Version 4 and Version 5 of Kerberos. 3
