IT 8-2 (RC)

B.E. IT (Semester – VIII) Examination, May/June 2012
COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY

Duration : 3 Hours | Total Marks : 100

Instructions : *1) Answer **five** questions in all selecting atleast **one** question from each Module.*
*2) Assume **missing** data **if** any.*

Module – I

1. a) Elaborate on any 8, X 800 security services. **8**

   b) With examples, describe the following multi-letter ciphers. **8**
   i) Playfair ii) Hill Cipher.

   c) Compare and differentiate nature audit records and detection specific audit records. **4**

2. a) Briefly explain the Rule Based Intrusion detection techniques. **6**

   b) Describe some of the issues in the design of a distributed Intrusion detection system. With an example, explain the architecture of a distributed IDS. **8**

   c) Define a virus. Describe the various phases in the lifetime of a virus. **6**

Module – II

3. a) Elaborate on some of the design features of the Feistel Cipher structure. **6**

   b) State the advantages of the counter block cipher mode of operation. **4**

   c) Compare Link to link and end to end encryption placement techniques. **8**

   d) State Fermats and Eulers theorem. **2**

4. a) Provide a brief overview of discrete logarithms in public key algorithms. **6**

   b) What is a product cipher ? Clearly explain the concept of diffusion and confusion in cryptographic systems. **6**

   c) For a user workstation in a typical business environment, list potential locations for confidentiality attacks. **6**

   d) What do you mean by Avalanche effect ? Does DES exhibit it ? **2**

P.T.O.

Module – III

5. a) Explain the RSA algorithm. Considering the 2 prime numbers to be II and 3, determine the private public key pair. **8**

   b) Explain the public key authority and public key certificates techniques for distribution of public keys. **8**

   c) What is a primitive root ? How is it calculated ? Is 2 a primitive root of 11. Justify your answer. **4**

6. a) Elaborate on any 2 approaches to producing message authentication. **8**

   b) Users A and B use the Diffie Helman key exchange technique with a common prime q = 71 and a primitive root $\alpha = 7$. **10**

      i) If user A has private key $X_A = 5$, what is A's public key Y_A ?

      ii) If user B has private key $X_B = 12$, what is B's public key Y_B ?

      iii) What is the shared secret key ?

   c) Define a Oneway Hash function. Where is it used ? **2**

Module – IV

7. a) Elaborate on Kerberos as an authentication service. **8**

   b) With a diagram, explain the X.509 authentication service. **6**

   c) Write a short note on S/MIME. **6**

8. a) Describe any 2 services provided by PGP. **8**

   b) Briefly describe the sequence of events that are required for a secure electronic transaction to purchase an item online. **6**

   c) Discuss the applications and limitations of firewalls. **6**