Roll No .....

MCSE-302(A)

M.E./M.Tech., III Semester

Examination, June 2014

Network Security (Elective-II)

Time : Three Hours

Maximum Marks : 70

Note: Total number of questions 8. Attempt five questions (including all parts). Assume missing data, if any, suitably.

1. a) What is the difference between a mono alphabetic and a poly alphabetic cipher? 7

   b) Explain how key distribution is achieved in symmetric key encryption. 7

2. a) Use a Hill cipher to encipher the message "We live in an insecure world". Use the following key. $K = \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$ 7

   b) List out the participants of SET system, and explain in detail. 7

3. a) Explain about the single round of DES algorithm. 7

   b) Define message authentication. Explain Message Authentication Code (MAC) and one way Hash Function. 7

4. a) Using play fair cipher algorithm encrypts the message using the key "MONARCHY" and explains. 7

   b) List hash function requirement and explain SHA-512. 7

5. a) In RSA given p = 19, q = 23, and e = 3, find all its parameters and explain the method by using suitable example. 7

   b) Explain briefly about Diffie Hellman key exchange algorithm with its pros and cons. 7

6. a) Explain two ways to achieve Digital Signature. Discuss, why does it not provide confidentiality? 7

   b) Using the DSS scheme, let q = 59, p = 709, and d = 14. Find values for e_1 and e_2. Choose r = 13. Find value for S_1 and S_2 if h(M) = 100. Verify the signature. 7

7. a) Define intruder. Name three different classes of intruders. 7

   b) Write in detail about definition, characteristics, types and limitations of firewalls. 7

8. a) Explain about viruses in detail. 7

   b) Explain HMAC with design objectives. 7

******