Total No. of Questions :8] *[Total No. of Printed Pages :2*

Roll No ....

MCSE-302(A)

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

Examination, December 2014

Network Security (Elective-II)

Time : Three Hours

Maximum Marks : 70

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

1. a) What is the difference between a differential and a linear cryptanalysis? 7

   b) Use a brute force attack to decipher the following message. Assume that you know it is an affine cipher and that the plaintext "ab" is enciphered to "GL" , message :-XPALASXYFGFUKPXUSOGEUTKCDGF. 7

2. a) Draw the table to show the results of passing 111111 through all 8 S-boxes. You see a pattern in the outputs?7

   b) Explain the Key Generation, Encryption and Decryption of SDES algorithm in detail. 7

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

   b) Explain briefly about RSA and discuss its merit. 7

4. a) In RSA, given n = 12091 and e = 13, Encrypt the message "THIS IS TOUGH " using the 00 to 26 encoding scheme. Decrypt the ciphertext to find the original message. 7

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

5. a) Explain any one mutual authentication mechanism with its advantages and drawbacks. 7

   b) Explain MD5 message digest algorithm in detail. 7

6. a) Write detail note on Internet Standard and internet Society. 7

   b) Explain authentication procedures in terms of x.509 7

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

   b) Define Network security and Data integrity. Differentiate between Kerberos version 4 and version 5. 7

8. a) Explain definition, Phases, types of virus structures and types of viruses. 7

   b) Describe the SSL Architecture in detail. 7

******