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

Roll No ....

MCSE-302(C)

M.E./M.Tech., III Semester Examination, June 2020

Network Security

(Elective-II)

Time : Three Hours

Maximum Marks : 70

Note: i) Attempt any five questions.
ii) All questions carry equal marks.

1. a) Explain about classical crypto systems (substitution and transposition) with two examples for each. 7

   b) With a neat block diagram, explain the network security model and the important parameters associated with it. 7

2. a) Differentiate active and passive security attacks. Categorize these attacks and explain one examples of each. 7

   b) Formulate the single round of DES algorithm and design the key discarding process of DES.7

3. Evaluate using Diffie-Hellman key exchange technique. Users A and B use a common prime q=11 and a primitive root alpha = 7. 14

   i) If user A has private key XA=3. What is A's public key YA?

   ii) If user B has private key XB=6. What is B's Public key YB?

   iii) What is the shared secret key? Also.

4. a) Draw the general structure of DES and describe how encryption and decryption are carried out and identify the strength of DES algorithm. 7

   b) Describe RSA algorithm and Estimate the encryption and decryption values for the RSA algorithm parameters. 7

5. a) Briefly describe the idea behind Elliptic Curve Cryptosystem and describe the key management of public key. 7

   b) Apply the mathematical foundations of RSA algorithm. Perform encryption decryption for the following data. P=17, q=7, e=5, n=119, message= "6". Use extended Euclid's algorithm to find the private key. 7

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

   b) Describe digital signature algorithm and show how signing and verification is done using DSS. 7

7. a) Compare and generalize the features of SHA and MD5 algorithm. 7

   b) Discuss the security of hash functions and MACs and describe any one method of efficient implementation of HMAC. 7

8. a) What are Viruses ? Explain the virus-related threats and the counter measures applied. 7

   b) Summarize about the authentication header of IP and discuss about encapsulating security payload of IP. 7

******