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

Roll No .....

MCSE-302(A)

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

Examination,December 2016

Network Security (Elective-II)

Time : Three Hours

Maximum Marks : 70

Note: Attempt any five questions. All questions carry equal marks.

1. a) In S-DES, 10-bit key is 1010000010. Find the subkeys k_1, and k_2, if

   P_{10} = 3 5 2 7 4 10 1 9 8 6 and

   P_8 = 6 3 7 4 8 5 10 9

   b) Explain the single round of DES encryption.

2. a) Define the elliptic curve over Zp. Write the corresponding addition formula.

   b) Discuss direct digital signatures and arbitrated digital signatures.

3. Write extended euclid algorithm and find the value of the following :

   a) $47^{1395} \bmod (48)$

   b) $4^{3207} \bmod (1024)$

   c) $2^{57} \bmod (123)$

4. a) Draw a neat diagram of IPSec ESP format and explain.

   b) Differentiate between network based. IDS and host based IDS emphasizing on their advantages and disadvantages.

5. a) What is a Firewall? List the type of firewalls. categorized by processing mode.

   b) Draw a schematic diagram of a packet-filtering router used as a firewall and explain its function using a sample firewall rule.

6. a) Give two examples of denial of service attack.

   b) State whether symmetric and asymmetric cryptographic algorithms need key exchange explain.

7. a) User A and B use Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root $\alpha = 7$. If user A has private key $X_A = 5$, what is A's public key Y_A.

   b) Explain RSA algorithm with example

8. a) Explain Kerberos authentication mechanism with suitable diagrams.

   b) With the help of block diagram, explain the process of public key exchange with the help of certificate authority.

******