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

Roll No ....

MCSE-302(A)

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

Examination, November 2018

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 Data encryption standard and the strength of DES in detail.

   b) Explain block Cipher design principles and various modes of operations.

2. a) Explain differential and linear cryptanalysis in detail.

   b) What is public key cryptography? Explain principles of public key cryptosystem.

3. a) What does encryption means? Discuss the Conventional Encryption Model in detail.

   b) In RSA algorithm, given p = 19, q = 23 and e = 3, find out the following:

   i) n ii) Φ(n)
   iii) d iv) Public key
   v) Private key

4. a) Define a cryptographic hash function. What are the properties of hash functions?

   b) If n = 17, g = 113. Secret numbers x = 3, y = 4. Then find the secret shared key using Diffie-Hellman key exchange algorithm.

5. a) Explain the following algorithms:

   i) MD5
   ii) SHA-1

   b) What are digital signatures? Write the applications of digital signature?

6. a) What is Kerberos? How does it work? Discuss with it detail requirement and applications?

   b) With the help of a suitable diagram, explain the operational procedure of SSL record protocol.

7. a) What is an Intruder? Explain the various classes of the Intruders.

   b) What is firewall? Explain design principles of firewall.

8. Write short notes (any four):

   a) HMAC digital signature
   b) RIPEMD
   c) Virus and worms
   d) SET
   e) Message Authentication

******