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

 Roll No .....

MCSE-302(A)

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

Examination, June 2017

Network Security

(Elective-II)

Time : Three Hours

Maximum Marks : 70

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

1. a) What is a stream cipher? How does it differ from permutation cipher? Describe with an example.
   b) Differentiate between Differential Cryptanalysis and Linear Cryptanalysis.

2. a) Write RSA algorithm for encryption and decryption for the given p = 3, q = 11, e = 7 and m = 5.
   b) Explain block cipher modes of operation.

3. a) Consider the Diffie-Hellman Scheme with a common prime q = 11 and primitive root $\alpha = 2$.
      i) show that 2 is indeed a generation.
      ii) if the user A has public key $Y_A = 9$ what A's private key.
      iii) if the user B has public key $Y_B = 3$ what is the secret key K in between A and B.
   b) Discuss the Vulnerabities of DES.

4. a) A lice is using a toy version of the DSS signature scheme with a prime modulus p =47 and generator g = 2 of order q = 23. By accident, slice generates signatures for two different messages with the same per message random number K. The hash codes of two signed messages are 2 and 3 and signatures are (4, 21) and (4, 19) respectively. Compute slice private key.
   b) Describe how a cryptographic hashing function can be implemented using a block cipher.

5. a) Discuss the strength of DES?
   b) List the characteristics of a good firewall implementation? How is a circuit gateway different from an application gateway?

6. a) Describe the role of Ticket granting server in Kerberos authentication protocol.
   b) What is the need of dual signature in SET? Describe with block diagram, how they are constructed.

7. a) Give the taxonomy of malicious programs? List the software threats and explain them.
   b) Explain SHA-I briefly.

8. Write short notes on the following:
   a) RIPEMD
   b) HMAC
   c) MD5
   d) Viruses and Related Threats.

******