

Total No. of Questions : 8]

[Total No. of Printed Pages : 2

Roll No

MCSE-302(A)
M.E./M.Tech., III Semester

Examination, December 2017

Network Security

(Elective-II)

Time : Three Hours

Maximum Marks : 70

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

1. a) What do you mean by steganography? Explain. Write drawbacks of encryption when compared to encryption.
 b) Explain simplified DES. What is the purpose of S-boxes in DES? Explain the Avalanche effect.
2. a) What do you mean by cryptanalysis? Differentiate linear and differential cryptanalysis.
 b) What are two most difficult problems of symmetric encryption? Write the characteristics of public key crypto systems.
3. a) What are the differences between conventional encryption and public key encryption?
 b) Explain the RSA algorithm with an example.
4. a) Briefly discuss Diffie-Hellman key exchange algorithm.
 b) What do you understand by message authentication code? Explain.

[2]

5. a) What is Hash function? Give the basic uses of Hash function.
 b) What basic arithmetical and logical functions are used in SHA-1 and MD5.
6. a) What is digital signature? Explain arbitrated and direct approach for digital signature.
 b) What was Kerberos designed for? Explain the architecture of Kerberos.
7. a) What is IP Security? What are the various merits of IP security?
 b) List and briefly define three classes of intruders. What are two common techniques used to protect a password file?
8. Write short notes on (any Two):
 a) Firewall design principles
 b) IP spoofing
 c) RANSOMWARE
 d) Brute force attacks

548