

d) Explain the different types of firewall configuration. What are the differences between the three configurations?

OR

What are intruders? Explain benefits that can be provided by an intrusion detection?

******

Roll No .....

MCA - 505(E)

MCA. V Semester

Examination, December 2015

Network Security

Elective-III

Time : Three Hours

Maximum Marks : 70

Note: i) Answer five questions. In each question part A, B, C is compulsory and D part has internal choice.

ii) All parts of each question are to be attempted at one place.

iii) All questions carry equal marks, out of which part A and B (Max. 50 words) carry 2 marks, part C (Max. 100 words) carry 3 marks, part D (Max. 400 words) carry 7 marks.

iv) Except numericals, Derivation, Design and Drawing etc.

Unit - I

1. a) What is steganography?

b) Differentiate between substitution technique and transposition technique?

c) Explain the concept of blowfish?

d) What are the block cipher modes of operation and discuss the techniques and applicability of differential and linear cryptanalysis in DES?

OR

During encrypting a message using DES in ciphertext block chaining mode, following error has occurred:

i) One bit of ciphertext in block C_i is accidentally transformed from a 0 to 1 during transmission. How much plaintext will be garbled as a result?

ii) One extra bit of ciphertext in block C_i is inserted during encryption. How much plaintext will be garbled?

Unit - II

2. a) Explain Euler's theorem.

b) What is public key encryption?

c) What is elliptic curve cryptography?

d) Briefly explain Diffie Hellman key exchange. The Diffie Hellman key exchange is being used to establish a secret key between 'A' and 'B'. 'A' send B (719, 3, 191), B responds with (543). 'A's secret number, X is 16. What is the secret key.

OR

In RSA encryption method, if the prime no. p and q are 3 and 7 respectively, the encryption exponent e is 11, find the following:

i) The least positive decryption exponent d.

ii) Public and private key

iii) Cipher text when the plain text P is encrypted using the public key.

Unit - III

3. a) What do you understand by authentication? State its requirements?

b) Explain Kerberos.

c) What are hash functions? How security is achieved by using them?

d) Briefly explain the difference between X5009 and PGP digital signature. List the major component of a digital certificate.

OR

Explain the following:

i) MD5

ii) RIPEMD-160

Unit - IV

4. a) Explain Pretty Good privacy.

b) What is the full form of MIME?

c) Explain the IP security architecture.

d) What are the various web security approaches? Briefly explain them.

OR

Explain the concept of IP security. What are the application and benefits of IP security?

Unit - V

5. a) Define virus and worms.

b) What are firewall design principles?

c) What are the threats associated with authentication?