OR

What is dual signature? Justify the importance of dual signature in SET (Secure Electronic Transaction).

**Unit - V**

5. a) Four techniques are used by firewall to control access and enforce security policies. Name them?

   b) Define attacks and threat?

   c) What are typical phases of operation of VIRUS?

   d) List the design goals and limitation for Firewall?

OR

What's the difference between a Packet level Firewall and an application layer Firewall?



******









**Roll No** .....

# MCA - 505(E)

## MCA V Semester

Examination, December 2014

## 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) NIST defines three key objectives of computer security, Name and define them briefly.

   b) What are the two basic functions used in encryption algorithms?

   c) What is a meet-in-the-middle attack?

   d) Draw the key generation logic of S-DES. Generate the set of sub keys in S-DES using key generation logic using (0111111101). Where the permutation boxes are defined as:

| P-10 | P-8 |
|---|---|
| 3 5 2 7 4 10 1 9 8 6 | 6 3 7 4 8 5 10 9 |

OR

What do you mean by modular arithmetic? Write the properties of congruence. Prove the followings:

i) $a = b \pmod n$ and $b = c \pmod n$ imply $c = a \pmod n$

ii) $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$

iii) $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

## Unit - II

2. a) What is primitive root? Find all possible primitive roots of 11.

b) What is an elliptic curve? What is the sum of three points on an elliptic curve that lies on straight line?

c) Define Fermat's Theorem? Use Fermat's theorem to find value of $3^{201} \bmod 11$.

d) Write Diffie-Hellman key exchange algorithm. Consider the algorithm scheme with common prime q = 11 and primitive root a = 2.

i) Show that 2 is the primitive root of 11.

ii) If user A has private key $X_A = 5$, what is its public value $Y_A$.

iii) If user B has private key $X_B = 12$, what is its public value $Y_B$.

iv) What is shred secret key K.











OR

Define RSA (Rivest Shamir And Adleman) algorithm for encryption and decryption. Show the computation for followings:

p = 7, q = 11, e = 17 and M = 8.

## Unit - III

3. a) What characteristics are needed in secure hash function?

b) What two levels of functionality comprise a message authentication or digital signature mechanism?

c) What problem was Kerberos designed to address?

d) List some of the threats associated with direct digital signature scheme. Also describe requirements should a digital signature scheme satisfy.

OR

Define the different steps of processing a message using SHA. Also draw the comparison between different versions of SHA.

## Unit - IV

4. a) What is difference between an SSL connection and SSL session?

b) Define the services provided by SSL record protocol.

c) What are the five principal services provided by PGP.

d) List the major security services provided AH (Authentication Header) and ESP (Encapsulating Security Payload) respectively?