Roll No. | | | | | | | | | | | | |

Total No. of Pages: 02

Total No. of Questions: 09

MCA (Sem.-5th)

NETWORK SECURITY & ADMINISTRATION

Subject Code: MCA-502

Paper ID: A3160

Time: 3 Hrs. **Max. Marks: 100**

INSTRUCTION TO CANDIDATES:-

Attempt FIVE Questions in all, including Q-9 in section-E, which is compulsory and selecting ONE each from Section-A to Section-D.

Section-A

Q1 a) Give model for Internetwork Security and explain different types of attacks. How are these attacks handled? **(10)**

b) What is Cipher block chaining (CBC)? Explain why chaining mode can prevent simple block swap attack for block ciphers such as AES and DES? **(10)**

Q2 a) What is the difference between block cipher and stream cipher? What are the different modes of block cipher operation? Explain any one of them.

b) What is the idea behind meet-in-the-middle attack? How it can be avoided in Triple DES? Explain by taking an example. **(10,10)**

Section-B

Q3 What do you mean by Public key Cryptography? Explain the RSA algorithm. Using this algorithm, if N =187 and the encryption key E=17, then find out the corresponding private key. **(20)**

Q4 a) Explain Kerberos in detail. How is reliability addressed in Kerberos? Why is time synchronization crucial in Kerberos? Suppose Company A deploys Kerberos on the network, what does Kerberos need to function properly?

b) Compare password based and certificate based authentication approach. Is mutual authentication the best way for authentication? **(10,10)**

Section-C

Q5. a) What is the working of a firewall? Explain different types of firewalls.

b) Explain the use of Network Address Translation (NAT) with the help of an example **(10,10)**

Q6. a) Explain IP Security Architecture. What is the purpose of authentication header? Explain the encapsulating security payload (ESP).

b) What services IPSec provides at network layer. Discuss in detail. **(10,10)**

Section-D

Q7. a) What is a Security socket Layer (SSL)? In a secured socket layer (SSL) connection, is the session-key chosen by the client or the server? How is it communicated to the other party?

b) The SSL protocol uses a Message Authentication Code (MAC) to authenticate data being sent over SSL. Why is a MAC chosen instead of a digital signature? What might be the benefit of using a digital signature rather than a MAC?

Q8. What is Requirement of Electronic Mail Security? How Electronic Mail security goals can be achieved? Explain the concept of PGP in Electronic mail security. **(20)**

Section-E (Compulsory Question)

Q9

a) What is man-in-the middle attack? Explain.
b) Encrypt the message "Hello world" using Play fair cipher with key "star".
c) What is Brute force Attack?
d) Define symmetric key encryption.
e) How can you differentiate authentication and authorization?
f) Disclosure is a threat against which security goal?
- i) Confidentiality
- ii) Integrity
- iii) Assurance
- iv) Availability

g) Which of the following most accurately defines vulnerability?
- i) A set of circumstances that has the potential to cause loss or harm.
- ii) Techniques for keeping data and resources hidden.
- iii) A weakness in the system that can be exploited to cause harm.
- iv) Techniques for detecting unexpected behavior

h) If all traffic that comes through the gateway is encrypted, how will it affect network level firewalls?
i) TRUE or FALSE: SSL and TLS provide essentially the same end-to-end security properties.
j) What is Requirement of Web Security? **(10×2=20)**

-----END-----