MASTER OF COMPUTER APPLICATION
Fifth Semester
INFORMATION SECURITY
(MCA - 22)

Duration: 3Hrs. **Full Marks: 70**

Part-A (Objective) =20
Part-B (Descriptive) =50

(PART-B: Descriptive)

Duration: 2 hrs. 40 mins. **Marks: 50**

Answer any *four* from *Question no.* 2 to 8
***Question no.* 1 is compulsory.**

1. What are the key principles of security? What is access control? How different is it from availability? (5+3+2=10)
2. Distinguish between Symmetric and Asymmetric Key Cryptography. Discuss the Diffie-Hellman key exchange algorithm with an example. (2+8=10)
3. Distinguish between stream and block ciphers. Explain the main concept in DES. (3+7=10)
4. What are the key requirements of message digests? Explain the basic principles of MD5. (3+7=10)
5. What do you mean by Public Key Cryptography? If A wants to send a message securely to B, what would be the typical steps involved? Write the RSA algorithm. (2+4+4=10)
6. Why should we trust digital certificate? What are the typical contents of a digital certificate? Give structure of a X.509V3 digital certificate. (2+3+5=10)
7. What do you mean by authentication? What is Kerberos? How does Kerberos work? (1+1+8=10)
8. What is the role of cyber law? What are their different types? Discuss the different types of cyber crime in details. (1+2+7=10)

*****

MASTER OF COMPUTER APPLICATION
Fifth Semester
INFORMATION SECURITY
(MCA - 22)

Duration: 20 minutes **Marks – 20**

(PART A - Objective Type)

I. Choose the correct answer: **1×20=20**

1. The language that we commonly used can be termed as……..
   A. pure text B. simple text
   C. plain text D. normal text

2. The codified language can be termed as……..
   A. clear text B. unclear text
   C. code text D. cipher text

3. Caesar Cipher is an example of ……..
   A. Substitution Cipher B. Transposition Cipher
   C. Substitution as well as Transposition Cipher D. None of the above

4. The principle of ……..ensures that only the sender and the intended recipients have access to the contents of a message.
   A. confidentiality B. Authentication
   C. integrity D. access control

5. If we want to ensure the principle of ……., the content of a message must not be modified while in transit.
   A. confidentiality B. Authentication
   C. integrity D. access control

6. Conversion of cipher text into plain text is called as……
   A. encryption B. decryption
   C. cryptography D. cryptanalyst

7. A digital certificate binds a user with……
   A. the user's private key B. the user's public key
   C. the user's passport D. the user's driving license

8. The …… of the user should never appear in a certificate.
   A. public key B. private key
   C. organization name D. name

9. ……., we have the concept of key rings.
   A. PEM B. SMTP C. PGP D. MIME

10.Virus is a computer……

A. file B. program
C. database D. network

11.A ..... can provide its users with meaningful and often sensitive information such as user account names and passwords.

A. packet sniffer B. IP Spoofing

12.IPSec provides security at the…… layer.

A. application B. Transport
C. network D. data link

13.Key management in IPSec is done by……

A. tunnel mode B. transport mode
C. ESP D. IKE

14.In…….. the IP header of the original packet is also encrypted.

A. only tunnel mode B. only transport mode
C. both tunnel mode and transport mode D. n mode

15.Determining the identity of a user is called as……..

A. authentication B. Authorization
C. confidentiality D. access control

16……is the most common authentication mechanism.

A. Smart card B. PIN
C. Biometrics D. Password

17.Kerberos provides for……

A. encryption B. SSO
C. remote login D. local login

18.In Kerberos, the server that allows users to access various applications/servers is called as…….

A. AS B. TGT C. TGS D. file server

19.Email security can be achieved by……

A. PEM protocol B. PGP protocol
C. S/MIME protocol D. all of the above

20.PEM allows for……security options.

A. 2 B. 3 C. 4 D. 5

*****