REV-01
MCA/01/05

2023/12

SET A

MASTER OF COMPUTER APPLICATION
THIRD SEMESTER (REPEAT)
CRYPTOGRAPHY AND NETWORK SECURITY
MCA-302

[USE OMR SHEET FOR OBJECTIVE PART]

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

Objective

Time: 30 mins. **Marks: 20**

Choose the correct answer from the following: ***1×20=20***

1. 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

2. Reconnaissance attacks consist of the following:
   a. Ip Address
   b. Data packets
   c. Ping sweeps
   d. Set of protocols

3. When two different message digest have the same value, it is called as:
   a. Attack
   b. Collision
   c. Hash
   d. Overflow

4. Packet sniffer will be detected by:
   a. DNS method
   b. ARP Method
   c. Ping method
   d. All above

5. The main difference between RSA and ECC is that:
   a. ECC offers same level of security
   b. ECC is highly mathematical
   c. Both a & b
   d. None of these

6. .....increases the redundancy of plain text.
   a. Confusion
   b. Diffusion
   c. Both a & b
   d. None of these

7. CPT stands for:
   a. Cisco Packet Tracer
   b. Current procedural Terminology
   c. Certified Packet Tracer
   d. Cyber packet Tracer

8. DES encrypts block of .....bits.
   a. 32
   b. 56
   c. 64
   d. 128

9. Which of the following step ensures that plain text is not vulnerable in block cipher mode?
   a. Encryption
   b. Round
   c. Initial
   d. Chaining

10. Packet sniffing is a technique to:
    a. Transfer data
    b. To Ping data
    c. Monitor the data packets
    d. Remove virus

11. To decrypt a message encrypted using RSA, we need the.....
    a. Sender's private key
    b. Receiver's private key
    c. Sender's public key
    d. Receiver's public key

12. Which one of the following can be considered as the class of computer threats?
    a. Dos Attack
    b. Phishing
    c. Soliciting
    d. Both a and c

13. Eavesdropping Network snooping and packet sniffing are:
    a. Snooping
    b. Listening
    c. Prying
    d. On communication is to capture protocol packets

14. In order to allow multiple hosts to communicate with a single external host without compromising on the IP address range, the router needs to add details of the ..... to its translation table.
    a. IP addresses
    b. Port numbers
    c. Protocol information
    d. External host

15. Determining the identity of a user is called as.....
    a. Authentication
    b. Authorization
    c. Confidentiality
    d. Access control

16. Kerberos provides for.....
    a. Encryption
    b. SSO
    c. Remote login
    d. Local login

17. SSL layer is located between..... and.....
    a. Transport layer, network layer
    b. Application layer, transport layer
    c. Data link layer, physical layer
    d. Network layer, data link layer

18. Which of the following is considered as optional in SSL?
    a. Server authentication
    b. Database authentication
    c. Application authentication
    d. Client authentication

19. The..... protocol is similar to SSL.
    a. HTTP
    b. HTTPS
    c. TLS
    d. SHTTP

20. OpenSSL is an open source implementation of SSL, used to resolve.....
    a. Buffer overflow
    b. Handshake error
    c. Buffer Splitting
    d. Data integration

-- --- --

(Descriptive)

Time : 2 hr. 30 mins. Marks : 50

[Answer question no.1 & any four (4) from the rest]

1. a) Explain the concept of Network security and its common types. 5+5=10
   b) Explain the common types of Network vulnerabilities with suitable diagram.
2. What is Firewall? Explain the functions of different types of Firewalls in network security. What are the limitations of Firewalls? 2+5+3=10
3. a) Explain how UNIX operating system maintains security being a multi-user system. 5+5=10
   b) Describe the processes of each round that are executed 10 times in AES encryption algorithms.
4. a) State few lines on following terms: 5
   i) Sniffing and IP snoffing
   ii) Spoofing
   iii) Firewalls
   iv) QoS
   v) DoS
   b) Explain the operation descriptions of PGP. 5
5. a) Define IpSec. What are possible attacks that can be addressed by IpSec? 5+5=10
   b) Write a short note on RSA algorithm.
6. a) Write down the steps of DES encryption algorithm. 5+5=10
   b) How SSL handshake protocol works for knowing server to its clients? Explain.
7. a) What is message digest? How MD5 works to address birthday attack? 5+5=10
   b) What is digital signature? How it differs from message digest?
8. a) Demonstrate the concept of kerberos key distribution center with suitable diagram. 6
   b) Expand the Secure socket layer with layer architecture outline. 4

= = *** = =