

Date:7-03-2022

Registration number:

ST. JOSEPH’S COLLEGE (AUTONOMOUS), BENGALURU-27

MSC Computer Science - I SEMESTER

**SEMESTER EXAMINATION: OCTOBER 2021**

**(Examination conducted in January - March 2022)**

**CS 7421 - Cyber Security**

Time- 2 ½ hrs Max Marks-70

This question paper contains three parts and four printed pages

**PART-A**

**Answer all the questions, each carries one mark. 1x15=15**

1.Processing or communication provided by a system to give a specific kind of

protection to system resource

a. Security attack

b. Security mechanism

c. Security service

d. Passive attack.

2. Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of ------------------

a. Cryptographic system

b. Decipher

c. Cryptanalysis

d. None

3. Use play fair symmetric algorithm and find the cipher for “PROUD JOSEPHITES” with the key MONARCHY

a. TO MV BK AP FL BF LK XA

b. TO MV BK AP FL BF KL XA

c. TO MV BK AP FL BE LK XA

d.None of the above

4. In CBC scheme, the relation between plain and cipher text is -----

a. Ci = Pi XOR SelectLeft (EK (ShiftLeft(Ci+1)))

b. Ci = Pi XOR SelectLeft (EK (ShiftRight(Ci-1)))

c. Ci = Pi XOR SelectLeft (EK (ShiftLeft(Ci-1)))

d. None

5. Network layer firewall works as a \_\_\_\_\_\_\_\_\_\_  
a) Frame filter  
b) Packet filter  
c) Content filter  
d) Virus filter

6. Which one of the following is not a higher –layer SSL protocol?  
a) Alert Protocol  
b) Handshake Protocol  
c) Alarm Protocol  
d) Change Cipher Spec Protocol

7.One of the most obvious places to put an IDS sensor is neat the firewall, where exactly in relation to the firewall is the most productive place

a. Outside the firewall

b. Inside the firewall

c. Neither inside nor outside

d. Both inside and outside

8. Which of the following usually observe each activity on the internet of the victim, gather all information in the background, and send it to someone else?

a. Malware

b. Spyware

c. Adware

d. All of the above

9. It is a multi-part worm that traveled on USB sticks and spread through Microsoft Windows computers

a. Stuxnet

b. Virus

c. Bots

d. Ransom

10. In the SSL Protocol, each upper layer message if fragmented into a maximum of \_\_\_\_\_\_\_\_\_\_ bytes.  
a) 216  
b) 232  
c) 214  
d) 212

11.IT Act2000 is introduced by

a. Kapil Prasad

b. Ravi Hedge

c. Ramvilas Paswan

d. Pramod Mahajan.

12.IT 2000 consists of –sections—chapters—schedules

a.94.1,6

b.84,13,12

c.44,11,3

d.94,13,4

13. An intricate environment that involves interactions between people, software, and services

a. Cyber space

b. Cyber law

c. Penal law

d. Hard disk

14. The process of preservation, identification, extraction, and documentation of computer evidence

a. .Digital computer

b. Digital Forensics

c. Analog system

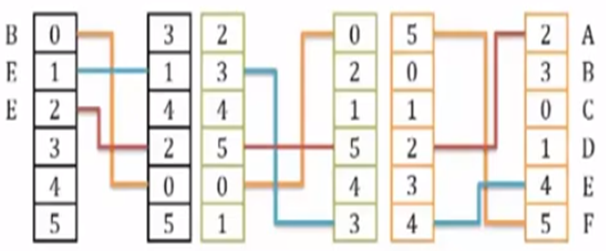
d. Digital media.

15. Which of the following is defined as an attempt to steal, spy, damage or destroy computer systems, networks, or their associated information?  
a. Cyber attack  
b. Computer security  
c. Cryptography  
d. Digital hacking

**Part-B**

**Answer all the five questions. Each question carries five marks. 5 x5=25**

16.a.What is symmetric Encryption and Explain Rail fence cipher, and what is the output of the following rotor machine



OR

b. Explain RSA algorithm, Find the value of ‘d’ when p=3 and q=11.

17 a. Differentiate IDS and IPS systems, According to you which is better to implement for security in big organizations.

OR

b. What is VPN, Mention any five tips to secure client VPNs.

18 a. What is SYN flood attack in TCP/IP.

OR

b. Why is cyber security important and how does it works.

19. a. What is cyber law, Write a short note on sections 43,66,67.

OR

b. What is the role of international law in cyber-crime?

20. a. What is Digital Forensics and what are the common situations where computer forensics is used.

OR

b. Explain Digital Forensics life cycle.

**PART C**

**Answer any three questions .Each carries ten marks 10X3=30**

21a. Explain DES algorithm in detail. Do we use same key for each round in DES [7+3]

b. Compare between CBC and CTR modes of operation.

22a.Expalin PGP cryptographic function for authentication. [4+6]

b. What is SHA and how SHA-1 works.

23a Write any three objectives to secure cyber ecosystem. [4+6]

b. Write a short note on a. firewalls and its types b. Hacker and types

24. Write a short note on [5+5]

a .Digital signature b. Block cipher principles.