D-1140

M. Sc. (I.T) (Fourth Semester) New
EXAMINATION, JUNE, 2020

Cyber Security
M. Sc. (I.T.) (401)

Time: Three Hours]   [Maximum Marks: 100

[Minimum Pass Marks:40

Note: Attempt all sections as directed.

SECTION – A

(Objective Type Questions,)

Note: Attempt all questions.   each 1 mark.

Q1 . Which is not job of antivirus software?

    A. Virus Detection   B. Virus Removal

    C. Storing Virus definition   D. Virus creation

Q2. Which is not type of an active attack?

    A. Traffic analysis   B. Replay

    C.   Denial of Service   D. Masquerade

Q3. Which is not an antivirus software?

    A. Net protector   B. Quick Heal

    C. Kali   D. Avast

Q4. Digital Signature is :

    A. Access Control Technique   B. An Authentication Technique

    C. Packet Filter Technique   D. None of the above

Q5. Wire Shark is :

    A. Anti Virus Software   B. Packet Analyzer Tool

    C. Firewall   D. Version of Linux

Q6. Which is not a terminology used in encryption technique.

    A. Plain Text   B. Cipher Text

    C. Encryption Algorithm   D. Big Text

Q7. Find the false statement related to security.

    A. Virus is kind of security threats

    B. Authentication, Access Control, Confidentiality, Integrity are described under security services.

    C. Cipher text meaning decrypted text

    D. Firewall Works as filter for packets

Q8. CFB stands for

    A. Cipher Feedback   B. Control Feedback

    C. Cipher Flow back   D. Control Flow back

Q9. An operating system dedicated to security services and applications is

    A. Windows 98   B. Kali Linux

    C. MS-Dos   D. Windows2000

Q10. IDS are

    A. Intruder Direction Security   B. Intruder Detector Services

    C . Intrusion Detection System   D. Intruder Destruction System

Q11. HMAC stands for :

    A. Hyper Mail Accounting Control

    B. Hashed Message Authentication Code

    C. Hashed Message Accounting Control

    D. Hyper Mail Authentication Code

Q12. Release of message contents is_____.

    A. Active Attack   B. Passive Attack

    C. Neither Active nor Passive   D. Both Active and Passive

Q13. OTP stands for

    A. On Time Payment   B. Over Traffic Protocol

    C. Over Time Policy   D. One Time Password

Q14. Availability ensures that

    A. Confidentiality of message

    B. System work promptly and services are not denied to authorized users

    C. Authenticity of user

    D. None of these

Q15. AES uses Block length of

    A. 256 bits   B. 128 bits

    C. 64 bits   D. 512 bits

Q16. What is the key size in DES algorithm

    A. 64 bit key   B. 32 bit key

    C . 16 bit key   D. 56 bit key

Q.17. RSA Encryption is a

    A. Symmetric Key Encryption Technique

    B. Public Key Encryption Technique

    C. Neither (A) nor (B)

    D. Both (A) and (B)

Q.18. Same keys are used in encryption as well as in decryption in

    A. Symmetric Key Encryption Technique

    B. Public Key Encryption Technique

    C. Neither (i) nor (ii)

    D. Both (i) and (ii)

Q.19. Which is not a usual strong password creation policy.

    A. It must be at least 8 characters long.

    B. It must contain numbers and special symbol.

    C. It must have at least one small letter and one capital letter

    D. It must contain your name or date of birth.

Q.20. DDos stands for

    A. Distributed Disk Operating System

    B. Divided Denial of service

    C. Distributed Denial of Service

    D. Divided Disk Operating System

SECTION – B
(Very Short Answer Type Questions)

Note: Attempt all questions. Answer using 2-3 sentences. each 2 marks

Q.1 What is Pseudorandom number?

Q.2 What is Crypt analysis?

Q.3 What is OAEP?

Q.4 What is RSA?

Q.5 What is finger printing?

Q.6 What is Process services ?

Q.7 What is virus?

Q.8 What is Honeypots?

Q.9 What is wireshark packet?.

Q.10 Why needed firewall in network?

SECTION – C

(Short Answer Type Questions)

Note: Attempt all questions. Answer precisely using <75 words.
each 3 marks.

Q.1 What do you mean by DOS attack?

Q.2. How many type of Security services?

Q.3. Explain the attacks on RSA.

Q.4. Write the security of hash function?

Q.5. What is difference between HMAC and CMAC?

Q.6. What do you understand by message digest?

Q.7. Write about the distributed intrusion detection.

Q.8 What is virus classification?

Q. 9 Write the various types of malicious software?

Q.10. What is firewall configuration.

SECTION – D

(Long Answer Type Questions)

Note: Attempt all question. Answer precisely using 150 words.
each 6 marks.

Q.1. What do you understand by Cyber Security? Explain the challenges of Computer Security.

OR

What do you mean by Symmetric Block Modes of operation? Explain the ECB, CBC, CFB and CTR

Q.2. Which type of approaches to use for messages authentication? Explain any one approach.

OR

What is cryptosystem? Write the applications for public key cryptosystem.

Q.3. What is the role of Hash function in message Integrity? Explain the Criteria random Oracle Model.

OR

What do you understand by Message Authentication? Explain the type of attacks on digital signature.

Q.4. What is Intrusion in malicious software? Explain any two Intrusion techniques

OR

Explain the following: -
(i)   Antivirus Approaches   (ii) Nature of Viruses

Q.5. What is the role of firewall? Write the characteristics of Firewall and type of firewall.

OR

Explain the following: -
(i)   Analyzer and its features   (ii) Domain of Cyber Security Policies

***