H-4/20/22 Roll No. ....

IV Semester Examination, 2022

M.Sc.

INFORMATION TECHNOLOGY

Paper I

(Cyber Security)

Time : 3 Hours] [Max. Marks : 100

Note : *All questions are compulsory. Question Paper comprises of 3 sections. Section **A** is objective type/multiple choice questions with no internal choice. Section **B** is short answer type with internal choice. Section **C** is long answer type with internal choice.*

SECTION A 1×10=10

(Objective Type/Multiple Type Questions)

Choose the correct answer :

1. Crash attack is a/an :

(a) The hackers exploit a bug on the server

(b) To create a ghost sever on the network

(c) Hacker sends a huge amount of traffic

(d) To hide malicious activity on the network

2. Salted hashes is a/an :

(a) Random data (b) Bug

(c) Blowfish (d) None of these

3. In public key cryptosystem .... keys are used for encryption and decryption.

(a) Same (b) Different

(c) Encryption Keys (d) None of the mentioned

4. What type of symmetric key algorithm using a streaming cipher to encrypt information ?

(a) RC4 (b) MD5

(c) SHA (d) Blowfish

5. When plain text is converted to unreadable format, it is termed as ....

(a) cipher-text (b) raw text

(c) rotten text (d) ciphen text

6. Cryptographic algorithms are based on mathematical algorithms where these algorithms use .... for a secure transformation of data :

(a) secret key (b) external programs

(c) add-ons (d) secondary key

7. Pretty good privacy program is used for :

(a) Electronic mails

(b) File encryption

(c) Electronic mails & File encryption

(d) None of the mentioned

8. What is the software called which when get downloaded on computer scans your hard drive for personal information and your internet browsing habits ?

(a) Backdoors (b) Key-logger

(c) Malware (d) Spyware

9. .... cryptography deals with traditional character,s *i.e.*, letters & digits directly.

(a) Modern (b) Classic

(c) Asymmetric (d) Latest

10. Sniffing is also known as ....

(a) network-tapping (b) wire-tapping

(c) net-tapping (d) wireless-tapping

SECTION B 6×5=30

(Short Answer Type Questions)

Unit-I

1. What do you mean by Application Security ? Explain the steps involved in securing Database.

Or

Explain the different approaches used for identifying and mitigating IT risks.

Unit-II

2. Briefly discuss applications for public key cryptosystem.

Or

Explain MITM attack and how to prevent it ?

Unit-III

3. Describe how a one-way hash function may be used for message authentication.

Or

Explain why a stream cipher fails to protect message integrity.

Unit-IV

4. Explain the difference between Virus, Worms and Trozan Horse.

Or

What is a Brute Force Attack ? How can you prevent it ?

Unit-V

5. Briefly discuss about Kali Linux with its architecture.

Or

Write short notes on Firewall Basing.

SECTION C 12×5=60

(Long Answer Type Questions)

Unit-I

1. What are AES, DES and triple DES different on the basis of design and features ? Also describe the operation of AES algorithm.

Or

Explain Symmetric Block Modes of operation with suitable example.

Unit-II

2. Write RSA algorithm in N = 187 and the encryption key E = 17. Find out the corresponding private key.

Or

What is Denial-of-Service attacks ? Discuss distributed Denial-of-Service attacks. How can one do defenses against Denial-of-Service attacks and how to respond to Denial-of-Service attack ?

Unit-III

3. The concept of computational complexity has superseded the notion of covertime as a measure of the security of a cryptosystem. Explain how computational complexity theory provides the theoretical basis for the design of modern scalable cryptosystems.

Or

What is digital signature ? Write the properties of digital signature and also list out the attacks related to digital signature.

Unit-IV

4. How can be Intrusion Detection system is the backbone of Information system ? Justify along with its categories.

Or

What is malicious software ? Discuss various malicious software with suitable example.

Unit-V

5. Explain the technical details of firewall and describe any three types of firewall with neat.

Or

Discuss Domain of cyber security Policies with real-time example.

✯ ✯ ✯ ✯ ✯ c ✯ ✯ ✯ ✯ ✯