Sl. No.	

A10.3-R5 Information Security Management

DURATION : 03 Hours **MAXIMUM MARKS : 100**

OMR Sheet No. :					

Roll No. : □□□□□□ **Answer Sheet No. :** □□□□□□

Name of Candidate : ______________________________ **; Signature of Candidate :** ____________________

INSTRUCTIONS FOR CANDIDATES :

- Carefully read the instructions given on Question Paper, OMR Sheet and Answer Sheet.
- Question Paper is in English language. Candidate has to answer in English language only.
- There are **TWO PARTS** in this Module/Paper. **PART ONE** contains **FOUR** questions and **PART TWO** contains **FIVE** questions.
- **PART ONE** is Objective type and carries **40** Marks. **PART TWO** is Subjective type and carries **60** Marks.
- **PART ONE** is to be answered in the **OMR ANSWER SHEET** only, supplied with the question paper, as per the instructions contained therein. **PART ONE** is **NOT** to be answered in the answer book for **PART TWO**.
- Maximum time allotted for **PART ONE** is **ONE HOUR**. Answer book for **PART TWO** will be supplied at the table when the Answer Sheet for **PART ONE** is returned. However, Candidates who complete **PART ONE** earlier than one hour, can collect the answer book for **PART TWO** immediately after handing over the Answer Sheet for **PART ONE** to the Invigilator.
- **Candidate cannot leave the examination hall/room without signing on the attendance sheet and handing over his/her Answer Sheet to the invigilator. Failing in doing so, will amount to disqualification of Candidate in this Module/Paper.**
- After receiving the instruction to open the booklet and before answering the questions, the candidate should ensure that the Question Booklet is complete in all respect.

DO NOT OPEN THE QUESTION BOOKLET UNTIL YOU ARE TOLD TO DO SO.

PART ONE

(Answer all the questions, each question carries ONE mark)

1. **Each question below gives a multiple choice of answers. Choose the most appropriate one and enter in the "OMR" answer sheet supplied with the question paper, following instructions therein.**

(1x10)

1.1 What is end-to-end delay in computer network communication ?

(A) Processing delay

(B) Transmission delay

(C) Propagation delay

(D) Sum of all above

1.2 Section 6 of ITA 2000 refers to :

(A) Legal recognition of evidence records

(B) Legal recognition of digital signatures

(C) Use of electronic records and digital signatures by the government and its agencies

(D) Retention of electronic records

1.3 What is Data espionage related to ?

(A) Cybercrime against person

(B) Cybercrime against property

(C) Cybercrime against nation

(D) All of these

1.4 Which of these is a group of volunteer-operated servers that allow users to improve their privacy on the network ?

(A) Tornetwork

(B) Peer-to-peer network

(C) Client-Server network

(D) Point-to-point network

1.5 Identification, acquisition, extraction, __________, evaluation, interpretation and presentation are the steps in forensic examination.

(A) precaution

(B) prevention

(C) preservation

(D) production

1.6 Acquisition can be done by which of the method/s ?

(A) Imaging

(B) Cloning

(C) Imaging and cloning

(D) Imaging or cloning

1.7 ACE refers to ___________.

(A) AccessData Certified Examiner

(B) Assistant Certified Examiner

(C) AccessSystem Certified Examiner

(D) Associate Certified Examiner

1.8 The characteristic of digital evidence is :

(A) visible

(B) time sensitive

(C) non-volatile

(D) unhandy

1.9 Which of the following requirement ensures that we cannot find messages that hash to same digest ?

(A) One-wayness

(B) Strong collision resistance

(C) Weak collision resistance

(D) Birthday attack resistance

1.10 Which of the following protocols operate in transport mode or the tunnel mode ?

(A) IPSec

(B) SSL

(C) PGP

(D) TLS

2. Each statement below is either TRUE or FALSE. Choose the most appropriate one and enter your choice in the "OMR" answer sheet supplied with the question paper, following instructions therein.
(1x10)

2.1 Any application using HTTP is always based on non-persistent connections.

2.2 802.1Q is an IEEE standard for frame tagging.

2.3 SMS spoofing is an SMS related crime wherein the attacker dupes the victims with messages to reveal their personal data.

2.4 Cyber extortion is a type of cybercrime against individual persons.

2.5 Volatile evidence analysis involves looking into connections, processes and cache tables.

2.6 Authentication Header provides either authentication or encryption or both for packets at IP level.

2.7 Encryption can be used to do hidden partitioning.

2.8 A data link layer security protocol provides end to end security services for applications.

2.9 Electronic evidence can't serve as accomplice and witness.

2.10 Cookies are dangerous as attackers emulate users by stealing their cookies.

3. **Match words and phrases in column X with the closest related meaning / word(s) / phrase(s) in column Y. Enter your selection in the "OMR" answer sheet supplied with the question paper, following instructions therein.**

(1x10)

X		Y	
3.1	Bridge	**A.**	Principal that determines minor changes to plaintext result into how many changes in ciphertext
3.2	Active attack	**B.**	A type of firewall configuration and placement
3.3	Avalanche Effect	**C.**	A technique used by attackers to fool users into revealing confidential information
3.4	Chosen Plaintext Attack	**D.**	Perpetrators taking control of a website by cracking administrative privileges
3.5	Demilitarized Zone	**E.**	Frames from one LAN can be transferred to other LAN using this device
3.6	Message Digest	**F.**	Form of attack where attacker attempts to change contents of message
3.7	Phishing	**G.**	Sending enormous amount of email messages to a server with intention to crash it
3.8	Certifying Authority	**H.**	Form of attack where attacker is able to get ciphertext of some plaintext of his choice
3.9	Webjacking	**I.**	Fingerprint of a message
3.10	Email Bombing	**J.**	A person who has been granted a license to issue digital signature certificate
		K.	One of the main application of Elliptic curve cryptography
		L.	Host based Intrusion detection system
		M.	Conversion of data into secured format

4. **Each statement below has a blank space to fit one of the word(s) or phrase(s) in the list below. Choose the most appropriate option, enter your choice in the "OMR" answer sheet supplied with the question paper, following instructions therein.** **(1x10)**

A.	Wannacry	**B.**	X.509	**C.**	ARP Module	**D.**	OS Fingerprinting
E.	SQLite	**F.**	Subpeona	**G.**	Email headers	**H.**	Circumstantial
I.	Anonymizer	**J.**	Physical	**K.**	Cyber laundering	**L.**	Open field
M.	TCP						

4.1 In __________ , the sending host takes any IP address on same LAN as input and returns its MAC address.

4.2 Indirect evidence is also known as __________ evidence.

4.3 __________ is a tool that attempts to make an activity on the Internet untraceable.

4.4 Better IP tracking is a preventive measure for __________ .

4.5 __________ was one of the largest ransomware based cyber attack.

4.6 __________ extraction is also called hex dump.

4.7 __________ compels the individual or organization that owns the computer system to surrender it.

4.8 8 email Tracker Pro is used to analyse __________.

4.9 __________ is an ITU-T standard for Public Key Infrastructure and Privilege Management Infrastructure.

4.10 Scanning a target network to detect operating system types is called __________.

PART TWO

(Answer any FOUR questions)

5. (a) Describe the standard security services to be provided by a secure information system.

(b) Explain computer security incident response goals and methodology.

(8+7)

6. (a) Detail the risk assessment process to define objective and scope of security audit.

(b) What is SQL injection attack ? How it can be used to illegally access database records ?

(10+5)

7. (a) Describe the key generation process of 128 bit AES algorithm with example.

(b) Explain the elliptic curve cryptosystems and their applications.

(8+7)

8. (a) Describe in detail the guidelines for issuing the Digital Signature Certificates by certifying authorities according to IT Act 2000. Include guidelines of generation, issuance and lifetime specifically.

(b) Explain forensic duplication, its requirements and forensic image formats.

(8+7)

9. Briefly explain the following (**Any three**).

(a) Worm Malware

(b) Application Proxy Firewall

(c) Link Encryption

(d) Heuristic Based Intrusion Detection System

(5x3)

- o O o -

SPACE FOR ROUGH WORK

SPACE FOR ROUGH WORK