No. of Printed Pages : **8**

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 respects.

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 attached to the question paper, following instructions therein.**

(1x10)

1.1 Which technique is used for increasing the redundancy of the plaintext ?

(A) confusion

(B) diffusion

(C) violation

(D) None of the above

1.2 Which key is required to decrypt the message at receiver side in public-key (asymmetric) cryptography ?

(A) public key

(B) private key

(C) plain key

(D) secret key

1.3 The cyberlaw of India is established in :

(A) August, 2000

(B) April, 2000

(C) January, 2000

(D) June, 2000

1.4 Which issue is not involved in IT act, 2000 ?

(A) Regulation of Certifying Authorities

(B) Law for E-Commerce

(C) Intellectual Property Rights

(D) License for Providing Internet Services

1.5 DNS run over :

(A) Port 80

(B) Port 21

(C) Port 53

(D) Port 32

1.6 The main purpose of data protection act is to :

(A) Protect personal privacy

(B) Prevent Viruses

(C) Increase the security of computer systems

(D) Reduce Project Failures

1.7 ACL stands for :

(A) actual control list

(B) access control list

(C) access cryptography list

(D) actual cryptography list

1.8 Which is **not** OWASP Vulnerabilities ?

(A) SQL Injection

(B) Malicious file execution

(C) Restricted URL access

(D) Broken Authentication and Session Management

1.9 In order to ensure the security of the data/information, we need to __________ the data :

(A) Decrypt

(B) Encrypt

(C) Delete

(D) Recover

1.10 The assessment process of a system does not include the identification and analysis of :

(A) all assets of and processes related to the system

(B) system vulnerabilities and the associated threats

(C) selection of appropriate security measures and analysis of the risk relationships

(D) system accuracy and the associated advantages

2. Each statement below is either TRUE or FALSE. Choose the most appropriate one and ENTER in the "OMR" sheet attached to the question paper, following instructions therein. (1x10)

2.1 A SQL injection attack consists of insertion of a SQL query through the input data from the client to the application.

2.2 The avalanche effect is a desirable property of cryptographic hashing algorithm when an input is changed slightly the output changes significantly.

2.3 The Data Encryption Standard (DES) technique uses 48 bit key.

2.4 Digital Signature provide certainty of date and time of electronic record.

2.5 The secure hash algorithm 1(SHA-1) is a hash algorithm that creates a 160-bit or 20-byte message digest.

2.6 MD5 checksum is a 64-bit value that helps identify the uniqueness of a file.

2.7 Access Control Violation threat arises from flagging HTTP cookies with tokens as secure.

2.8 Dictionary attack can force a user's session credential or session ID to an explicit value.

2.9 The employee makes statements relating to things they personally saw or took part in, can be taken as evidence for security audit.

2.10 The sample does not need to be statistically based for security audit.

3. **Match words and phrases in column X with the closest related meaning/word(s)/phrases in column Y. Enter your selection in the "OMR" answer sheet attached to the question paper, following instructions therein. (1x10)**

X		Y	
3.1	Network Layer device	**A.**	Security Risk Assessment
3.2	Hiding the information within data.	**B.**	Security Audit
3.3	Focus on the risk perspective, assessment areas not necessarily related to security policies and standards	**C.**	AND
3.4	Focus on the compliance perspective, assess against security policies, standards or other pre-defined criteria	**D.**	Steganography
3.5	It is a group of network devices (computers, servers, and other resources) that behave as if they are connected to a single network segment, even though they might not be.	**E.**	Router
3.6	Network device at Physical layer	**F.**	VLAN
3.7	Act of Cyber Terrorism	**G.**	Hub
3.8	simple encryption often used by an intruder or criminal	**H.**	Section 66F
3.9	Example of symmetric encryption	**I.**	RSA
3.10	Changing of data before or during entry into the computer system	**J.**	ELAN
		K.	XOR (exclusive OR)
		L.	Data Diddling
		M.	DES

4. **Each statement below has a blank space to fit one of the word(s) of phrases in the list below. Enter your choice in the "OMR" answer sheet attached to the question paper, following instructions therein.** **(1x10)**

A.	15	**B.**	X.500	**C.**	Vigenere	**D.**	Static routing
E.	MD5	**F.**	Open Web Application Security Project	**G.**	threat	**H.**	Data integrity
I.	X.509	**J.**	16	**K.**	vulnerability	**L.**	Trojans
M.	Open Web Assessment Security Project						

4.1 __________ is the manual configuration and selection of a network route, usually managed by the network administrator.

4.2 __________ is the accuracy, completeness, and reliability of data throughout its lifecycle.

4.3 __________ is a series of computer networking standards covering electronic directory services.

4.4 The program that act like something useful but do the things that are quiet damping is known as __________.

4.5 A __________ is a weakness in the system.

4.6 A __________ is the possibility of an attack

4.7 OWASP stands for __________.

4.8 The __________ algorithm is a widely used hash function producing a 128 bit hash value.

4.9 The largest number of hops allowed for RIP (Routing Information Protocol) is __________.

4.10 __________ cipher is a poly-alphabetic substitution system that use a key and a double-entry table.

SPACE FOR ROUGH WORK

PART TWO

(**Answer any FOUR questions**)

5. (a) Explain network topology in brief.

(b) Differentiate between TCP and UDP Protocols.

(c) Explain the function of WiFi and Bluetooth in detail.

(6+4+5)

6. (a) What is a firewall ? Explain types of firewall.

(b) List the phases in hacking and explain each in brief.

(c) Which are the properties of hash function ?

(5+6+4)

7. (a) Explain the types of cyber-attacks in brief.

(b) Explain Diffie - Hellman key exchange algorithm.

(9+6)

8. (a) What is symmetric key cryptography ? What are the challenges of symmetric key cryptography ? List out various symmetric key algorithms.

(b) What is an Intrusion Detection Systems ? Write differences between NIDS and HIDS.

(c) Explain Risk-based audit planning stages.

(5+5+5)

9. (a) What is cross-site scripting (XSS) ? And how to prevent it ?

(b) What is Cybercrime ? Explain various categories of Cybercrimes.

(c) Explain digital forensic process.

(5+5+5)

- o O o -

SPACE FOR ROUGH WORK

SPACE FOR ROUGH WORK