

Sl. No.

**A10.3-R5 : INFORMATION SECURITY MANAGEMENT**अवधि : 03 घंटे  
DURATION : 03 Hoursअधिकतम अंक : 100  
MAXIMUM MARKS : 100ओएमआर शीट सं. :   
OMR Sheet No. :रोल नं. :   
Roll No. :उत्तर-पुस्तिका सं. :   
Answer Sheet No. :परीक्षार्थी का नाम : \_\_\_\_\_;Signature of Candidate : \_\_\_\_\_  
Name of Candidate :**परीक्षार्थियों के लिए निर्देश :****Instructions for Candidate :**

कृपया प्रश्न-पुस्तिका, ओएमआर शीट एवं उत्तर-पुस्तिका में दिये गए निर्देशों को ध्यानपूर्वक पढ़ें।	Carefully read the instructions given on Question Paper, OMR Sheet and Answer Sheet.
प्रश्न-पुस्तिका की भाषा अंग्रेजी है। परीक्षार्थी केवल अंग्रेजी भाषा में ही उत्तर दे सकता है।	Question Paper is in English language. Candidate can answer in English language only.
इस मॉड्यूल/पेपर के दो भाग हैं। भाग एक में चार प्रश्न और भाग दो में पाँच प्रश्न हैं।	There are TWO PARTS in this Module/Paper. PART ONE contains FOUR questions and PART TWO contains FIVE questions.
भाग एक "वैकल्पिक" प्रकार का है जिसके कुल अंक 40 हैं तथा भाग दो "व्यक्तिपरक" प्रकार का है और इसके कुल अंक 60 हैं।	PART ONE is Objective type and carries 40 Marks. PART TWO is Subjective type and carries 60 Marks.
भाग एक के उत्तर, ओएमआर उत्तर-पुस्तिका पर ही दिये जाने हैं। भाग दो की उत्तर-पुस्तिका में भाग एक के उत्तर नहीं दिये जाने चाहिए।	PART ONE is to be answered in the OMR ANSWER SHEET only. PART ONE is NOT to be answered in the answer book for PART TWO.
भाग एक के लिए अधिकतम समय सीमा एक घण्टा निर्धारित की गई है। भाग दो की उत्तर-पुस्तिका, भाग एक की उत्तर-पुस्तिका जमा कराने के पश्चात् दी जाएगी। तथापि, निर्धारित एक घंटे से पहले भाग एक पूरा करने वाले परीक्षार्थी भाग एक की उत्तर-पुस्तिका निरीक्षक को सौंपने के तुरंत बाद, भाग दो की उत्तर-पुस्तिका ले सकते हैं।	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.
परीक्षार्थी, उपस्थिति-पत्रिका पर हस्ताक्षर किए बिना और अपनी उत्तर-पुस्तिका, निरीक्षक को सौंपे बिना, परीक्षा हॉल/कमरा नहीं छोड़ सकते हैं। ऐसा नहीं करने पर, परीक्षार्थी को इस मॉड्यूल/पेपर में अयोग्य घोषित कर दिया जाएगा।	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.
प्रश्न-पुस्तिका को खोलने के निर्देश मिलने के पश्चात् एवं उत्तर लिखना आरम्भ करने से पहले उम्मीदवार जाँच कर यह सुनिश्चित कर लें कि प्रश्न-पुस्तिका प्रत्येक दृष्टि से संपूर्ण है।	After receiving the instruction to open the booklet and before starting to answer the questions, the candidate should ensure that the Question Booklet is complete in all respect.

जब तक आपसे कहा न जाए, तब तक प्रश्न-पुस्तिका न खोलें।

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

**PART ONE**

**(Answer all the questions)**

**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 the protocol data unit (PDU) for the data link layer in the TCP/IP stack ?

- (A) Segment
- (B) Packet
- (C) Frame
- (D) Datagram

**1.2** The risk associated with cyber law can be minimized by :

- (A) introduction of authentication aspects
- (B) gathering information about criminals
- (C) focusing on cloud computing
- (D) all of these

**1.3** Which key(s) is used to verify a digital signature ?

- (A) Private Key
- (B) Public Key
- (C) Key pairs
- (D) Hash Key

**1.4** What term is used for unauthorized use, copy, or distribution of software ?

- (A) Software Crack
- (B) Trademark offence
- (C) Software Piracy
- (D) Clone

**1.5** \_\_\_\_\_ enables attackers to gain control over the computer by exploiting the vulnerabilities in the software.

- (A) Web jacking
- (B) XSS Attack
- (C) Theft of FTP Password
- (D) Exploit Kits

**1.6** Which malware produces multiple copies of itself in a way that all cannot be detected by virus scanners ?

- (A) Slow infector
- (B) Stealth virus
- (C) Polymorphic Virus
- (D) Worms

**1.7** What is the other term used for CEO Attacks ?

- (A) Pharming
- (B) Spear Phishing
- (C) Deceptive Phishing
- (D) Whaling

1.8 \_\_\_\_\_ the affected computer immediately and \_\_\_\_\_ if the computer is not fully affected.

- (A) Isolate, Restart
- (B) Isolate, hibernate
- (C) Isolate, power off
- (D) Integrate, restart

1.9 Which one is an electronic discovery technique used to determine and reveal technical criminal evidence ?

- (A) Cyber forensics
- (B) Cyber analysis
- (C) Digital evidence
- (D) None of these

1.10 How many phases are present to achieve national cyber security ?

- (A) 4
- (B) 6
- (C) 5
- (D) 7

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 Cyclic Redundancy Check is an error correction method.

2.2 RSA is a popular asymmetric key cryptography.

2.3 Different CAs can interoperate directly with each other for wider certification.

2.4 SSL provides both confidentiality and integrity services between client and server.

2.5 Two-factor authentication requires user to remember two passwords to access an account.

2.6 IPSec provides security between Internet and data link layers.

2.7 Statistical anomaly and rule based are two types of IDS.

2.8 A honeypot is a trap that attracts potential attackers.

2.9 Stateful packet filter examines incoming traffic using set of predefined rules.

2.10 Forensic copying includes creating an exact bit stream copy of original storage media of subject's computer.

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	OSPF	A.	A small useful program that has a hidden malicious program in it
3.2	Network Address Translation	B.	An ideal cipher with non-repeating key
3.3	RC5	C.	Documentation containing a list of people who were in possession of evidence
3.4	Secure Hash Algorithm	D.	Technology for implementing asymmetric key cryptography ecosystem
3.5	VPN	E.	A protocol for Intra-Autonomous system routing in the Internet
3.6	PGP	F.	Technology that makes use of public Internet as private network
3.7	Trojan Horse	G.	A standard for creating message digest
3.8	PKI	H.	It enables private IP networks that use unregistered IP addresses to connect to the Internet.
3.9	Vernam Cipher	I.	Symmetric key block encryption algorithm with variable length keys
3.10	Chain of custody	J.	Protocol for secure email communication
		K.	Password Guess Protocol
		L.	Used for communicating between two identical layers
		M.	Private Key Interface

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	CSIRT	B	write-blocker	C	socket	D	CCE
E	Cert-In	F	Star Configuration	G	Sandboxing	H	Black hat
I	hidden and swap	J	Sniffer	K	Delusional	L	Auto-configuration
M	Symmetric						

- 4.1 A network topology in which all data passes through a central system is called \_\_\_\_\_.
- 4.2 An endpoint of transport layer level communication flow is called \_\_\_\_\_.
- 4.3 \_\_\_\_\_ removes the dependability of DHCP servers.
- 4.4 An eavesdropping program to record all incoming and outgoing data is called \_\_\_\_\_.
- 4.5 \_\_\_\_\_ is a nodal agency setup to respond to computer security incidents.
- 4.6 \_\_\_\_\_ hackers identify and exploit system vulnerabilities.
- 4.7 AES is an example of \_\_\_\_\_ cryptography.
- 4.8 Anti-virus software implement \_\_\_\_\_ to create virtual machines to test untrusted files.
- 4.9 The contents of all \_\_\_\_\_ files are revealed as a result of forensics.
- 4.10 Analysts should use \_\_\_\_\_ to avoid introduction of data from other source.

## PART TWO

(Answer any FOUR questions)

5. (a) Give definition and explain types of active and passive attacks on systems with suitable examples. (8)
- (b) Describe the stages of digital forensic investigation. (7)
6. (a) Describe types, techniques and tools of evidence gathering used during security audit. (10)
- (b) What is cross site scripting attack ? Discuss persistent and non-persistent cross site scripting. (5)
7. (a) Explain asymmetric encryption with RSA with the help of an example. Detail the encryption, decryption and key generation process. (10)
- (b) What is a stream cipher ? List the important design considerations for its implementation ? (5)
8. (a) Describe the definition, creation, verification and standards to be used for digital signatures according to IT Act 2000. (8)
- (b) What is cyber warfare ? What are the critical issues associated with it ? Explain by quoting some instances of it. (7)

9. Briefly explain the following (Any three) :

- (a) Worm Malware
- (b) Network Flooding attacks
- (c) End-to-End Encryption
- (d) Signature Based Intrusion Detection System (5x3)

- o O o -

---

SPACE FOR ROUGH WORK

---

SPACE FOR ROUGH WORK