A 10.3-R5 INFORMATION SECURITY MANAGEMENT

अवधि : 03 घंटे **अधिकतम अंक : 100**
DURATION : 03 Hours **MAXIMUM MARKS : 100**

ओएमआर शीट सं. : **OMR Sheet No. :**						

रोल नं. : **Roll No. :** | | | | | | |

उत्तर-पुस्तिका सं. : **Answer Sheet No. :** | | | | | | |

परीक्षार्थी का नाम : **परीक्षार्थी के हस्ताक्षर :**
Name of Candidate : _____ ; **Signature of Candidate :** _____

परीक्षार्थियों के लिए निर्देश :	**Instructions for Candidates :**
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 अंग्रेजी भाषा में है। परीक्षार्थी उत्तर लिखने के लिए केवल अंग्रेजी भाषा का ही प्रयोग कर सकते हैं।	Question Paper is in English language. Candidate has to 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** है तथा **भाग दो** ''व्यक्तिपरक'' प्रकार का है और इसके कुल अंक **60** है।	**PART ONE** is Objective type and carries **40** Marks. **PART TWO** is Subjective type and carries **60** Marks.
भाग एक के उत्तर, इस प्रश्न-पत्र के साथ दी गई **ओएमआर उत्तर-पुस्तिका** पर, उसमें दिये गए अनुदेशों के अनुसार 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, 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**.
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 यह जाँच कर 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 An asymmetric-key (or public-key) cipher uses

(A) 1 Key

(B) 2 Key

(C) 3 Key

(D) 4 Key

1.2 Which algorithm among-MARS, Blowfish, RC6, Rijndael and Serpent -was chosen as the AES algorithm ?

(A) MARS

(B) Blowfish

(C) RC6

(D) Rijndael

1.3 What was the security algorithm defined for the IEEE 802.11 ?

(A) WEP

(B) RSN

(C) RSA

(D) SSL

1.4 Which of the following is false with respect to TCP ?

(A) Connection-oriented

(B) Process-to-process

(C) Transport layer protocol

(D) Unreliable

1.5 Which of the following malicious program do not replicate automatically ?

(A) Trojan Horse

(B) Virus

(C) Worm

(D) Zombie

1.6 Which is not the purpose of Risk analysis ?

(A) It supports risk based audit decisions

(B) Assists the Auditor in determining Audit objectives

(C) Ensures absolute safety during the Audit

(D) Assists the Auditor in identifying risks and threats

1.7 The objectives of IT audit include

(A) Ensures asset safeguarding

(B) Ensures that the attributes of data or information are maintained

(C) Both (A) and (B)

(D) None of the above

SPACE FOR ROUGH WORK

1.8 Which is not an attribute of CIA ?

(A) Availability

(B) Integrity

(C) Confidentiality

(D) Authentication

1.9 Under which section of IT Act, stealing any digital asset or information is considered a cyber-crime.

(A) 65

(B) 65-D

(C) 67

(D) 70

1.10 Which of the following is a Wireless traffic Sniffing tool ?

(A) Maltego

(B) BurpSuit

(C) Nessus

(D) Wireshark

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

2.1 An algorithm used in encryption is referred to as cipher.

2.2 Application layer sends & receives data for particular applications using Hyper Text Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP).

2.3 Application level gateway firewalls are not used for configuring cache-servers.

2.4 XSS stands for XML Site Server

2.5 ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an information security management system (ISMS).

2.6 Bluetooth uses time division multiplexing

2.7 Nessus is a remote security scanning tool

2.8 The chain of custody is established whenever an investigator takes custody of evidence at a crime scene.

2.9 UDP is transport layer protocol

2.10 Trojan Horse cannot do anything until actions are taken to activate the file attached by the malware.

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)

Column X		Column Y	
3.1	AES	A.	Wireless technology standard
3.2	Cross Site Scripting	B.	Asymmetric Key Cryptography
3.3	Phishing	C.	Symmetric Key Cryptography
3.4	Bluetooth	D.	Acts of cyberterrorism
3.5	S/MIME	E.	Failure to maintain records
3.6	RSA	F.	Routing Protocol
3.7	66F	G.	Fraudulent attempt to obtain sensitive information
3.8	67C	H.	Client-side code injection attack
3.9	Copyright	I.	Technology that allows you to encrypt your emails
3.10	RIP	J.	Exclusive right given to the creator of a creative work
		K.	Blockchain technology
		L.	Hshing Algorithm
		M.	Digital Signature Scheme

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

A.	buffer	**B.**	2008	**C.**	Router	**D.**	128 bits
E.	4-way handshake	**F.**	Decryption	**G.**	Access Point	**H.**	5
I.	56 bits	**J.**	6	**K.**	Encryption	**L.**	2010
M.	48 bits						

4.1 When a wireless user authenticates to any AP, both of them go in the course of four-step authentication progression which is called _____.

4.2 _____ is the central node of 802.11 wireless operations.

4.3 AES encryption key size is _____ bits

4.4 DES encryption key size is _____ bits

4.5 Packet filtering firewalls are deployed on _____.

4.6 A _____ is a sequential segment of the memory location that is allocated for containing some data such as a character string or an array of integers.

4.7 In which year the Indian IT Act, 2000 got updated? _____.

4.8 The section _____ deals with legal recognition of digital signature

4.9 The section _____ deals with the use of electronic records and digital signature in Government and its agencies

4.10 A process of making the encrypted text readable again is _____.

PART TWO

(Answer any **FOUR** questions)

5. (a) What is VLAN ? Explain the working of Inter VLAN routing in detail.

(b) Explain RSA algorithm. **(8+7)**

6. (a) Explain Network based IDS System.

(b) What is a firewall? List different types of firewall.

(c) What is the Diffie-Hellman key exchange and how does it work ? **(6+3+6)**

7. (a) What are OWASP top ten vulnerabilities ? Explain Cross site scripting in detail

(b) What is organizational risk management? What are the Risk Management steps ?

(c) What is the ISO 27001 standard? What are domains of ISO 27001 ? **(5+5+5)**

8. (a) What do you mean by Information Technology Act 2000? What are the main features of IT Act 2000 ?

(b) Explain each component of SSL X.509 certificate. **(8+7)**

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

(a) Digital evidence

(b) Audit planning

(c) SQL Injection

(d) Domain name dispute

(e) PKI

(f) HMAC **(5x3)**

- o O o -

SPACE FOR ROUGH WORK

SPACE FOR ROUGH WORK