Roll. No. ....

O.M.R. Serial No. | | | | | | | | |

Question Booklet Number

B.Sc. (SEM.-V) (NEP) (SUPPLE.)EXAMINATION, 2024-25

BIOTECHNOLOGY

(Information Security & Cyber Law)

Paper Code							
B	1	8	0	5	0	2	T

Question Booklet Series
A

Time : 1 : 30 Hours **Max. Marks : 75**

Instructions to the Examinee :

1. Do not open the booklet unless you are asked to do so.
2. The booklet contains 100 questions. Examinee is required to answer 75 questions in the OMR Answer-Sheet provided and not in the question booklet. All questions carry equal marks.
3. Examine the Booklet and the OMR Answer-Sheet very carefully before you proceed. Faulty question booklet due to missing or duplicate pages/questions or having any other discrepancy should be got immediately replaced.
4. Four alternative answers are mentioned for each question as - A, B, C & D in the booklet. The candidate has to choose the correct / answer and mark the same in the OMR Answer-Sheet as per the direction :

(Remaining instructions on last page)

परीक्षार्थियों के लिए निर्देश :

1. प्रश्न-पुस्तिका को तब तक न खोलें जब तक आपसे कहा न जाए।
2. प्रश्न-पुस्तिका में 100 प्रश्न हैं। परीक्षार्थी को 75 प्रश्नों को केवल दी गई OMR आन्सर-शीट पर ही हल करना है, प्रश्न-पुस्तिका पर नहीं। सभी प्रश्नों के अंक समान हैं।
3. प्रश्नों के उत्तर अंकित करने से पूर्व प्रश्न-पुस्तिका तथा OMR आन्सर-शीट को सावधानीपूर्वक देख लें। दोषपूर्ण प्रश्न-पुस्तिका जिसमें कुछ भाग छपने से छूट गए हों या प्रश्न एक से अधिक बार छप गए हों या उसमें किसी अन्य प्रकार की कमी हो, उसे तुरन्त बदल लें।
4. प्रश्न-पुस्तिका में प्रत्येक प्रश्न के चार सम्भावित उत्तर- A, B, C एवं D हैं। परीक्षार्थी को उन चारों विकल्पों में से सही उत्तर छाँटना है। उत्तर को OMR उत्तर-पत्रक में सम्बन्धित प्रश्न संख्या में निम्न प्रकार भरना है :

(शेष निर्देश अन्तिम पृष्ठ पर)

1.	Which policy ensures that personal information of users is protected on the web? a) Security Policy b) Privacy Policy c) Accessibility Policy d) Copyright Policy	1.	कौन-सी पॉलिसी यह सुनिश्चित करती है कि वेब पर उपयोगकर्ताओं की व्यक्तिगत जानकारी सुरक्षित रहे? a) Security Policy b) Privacy Policy c) Accessibility Policy d) Copyright Policy
2.	A strong password should include: A. Only letters B. Your name and birthday C. Letters, numbers, and special characters D. Simple and easy words	2.	एक मजबूत पासवर्ड में क्या शामिल होना चाहिए? A. केवल अक्षर B. आपका नाम और जन्मदिन C. अक्षर, संख्याएँ और विशेष वर्ण D. आसान और साधारण शब्द
3.	What does SPAM in emails usually refer to? a) Encrypted emails b) Unwanted or unsolicited bulk messages c) Secure mail protocols d) Email attachments	3.	ईमेल में SPAM आमतौर पर किसे दर्शाता है? a) एन्क्रिप्टेड ईमेल b) अनचाहे या बिना माँगे भेजे गए समूह संदेश c) सुरक्षित मेल प्रोटोकॉल d) ईमेल अटैचमेंट्स
4.	Which component of information security ensures that data remains complete, consistent, and accurate? a) Confidentiality b) Integrity c) Availability d) Authentication	4.	सूचना सुरक्षा का कौन-सा घटक यह सुनिश्चित करता है कि डेटा पूरा, सुसंगत और सही बना रहे? a) गोपनीयता b) अखंडता c) उपलब्धता d) प्रमाणीकरण
5.	Which of the following best ensures integrity of data? a) Hash functions and checksums b) Strong passwords c) Data encryption d) Multi-factor authentication	5.	डेटा की अखंडता (Integrity) को सबसे अच्छे से कौन सुनिश्चित करता है? a) हैश फ़ंक्शन और चेकसम b) मज़बूत पासवर्ड c) डेटा एन्क्रिप्शन d) मल्टी-फैक्टर ऑथेंटिकेशन

6.	In passive attacks, the attacker: a) Modifies system resources b) Steals passwords by brute force c) Only observes communication without changing it d) Shuts down servers	6.	पैसिव अटैक में अटैकर क्या करता है? a) सिस्टम रिसोर्सेज़ को बदलता है b) पासवर्ड चुराने के लिए ब्रूट फोर्स करता है c) सिर्फ कम्युनिकेशन को देखता है, बदलता नहीं d) सर्वर बंद कर देता है
7.	The goal of an active attack is to: A. Protect the system B. Encrypt files C. Change, disrupt, or damage data D. Scan for viruses	7.	एक एक्टिव अटैक का उद्देश्य क्या होता है? A. सिस्टम की सुरक्षा B. फाइल्स को एन्क्रिप्ट करना C. डेटा को बदलना, बाधित करना या नुकसान पहुंचाना D. वायरस स्कैन करना
8.	Denial of Service (DoS) is an example of: a) Active attack b) Passive attack c) Replay attack d) Traffic analysis	8.	Denial of Service (DoS) किसका उदाहरण है? a) Active attack b) Passive attack c) Replay attack d) Traffic analysis
9.	The most important step in system hacking is: a) Cracking passwords b) Covering tracks c) Information gathering d) None of the above	9.	सिस्टम हैकिंग में सबसे महत्वपूर्ण चरण कौन-सा है? a) पासवर्ड क्रैक करना b) ट्रैक छुपाना c) जानकारी इकट्ठा करना d) इनमें से कोई नहीं
10.	Which of the following is NOT a type of information system? a) TPS b) MIS c) DSS d) GPS	10.	निम्न में से कौन-सा सूचना प्रणाली (Information System) का प्रकार नहीं है? a) TPS b) MIS c) DSS d) GPS
11.	Which term refers to making data unreadable to unauthorized users? A. Formatting B. Encryption C. Compression D. Downloading	11.	उस प्रक्रिया को क्या कहते हैं जिसमें डेटा अनधिकृत उपयोगकर्ताओं के लिए पढ़ने योग्य नहीं होता? A. फॉर्मेटिंग B. एन्क्रिप्शन C. कंप्रेशन

			D. डाउनलोडिंग
12.	In Caesar cipher, if the shift is 3, what is the ciphertext for the plaintext “CAT”? a) FDW b) ZXP c) DBU d) FYT	12.	सीज़र सिफर में, अगर शिफ्ट 3 है, तो "CAT" का सिफरटेक्स्ट क्या होगा? a) FDW b) ZXP c) DBU d) FYT
13.	What is the primary reason businesses need cybersecurity? a) To increase internet speed b) To protect information assets and ensure business continuity c) To reduce the number of employees d) To avoid using encryption	13.	व्यवसायों को साइबर सुरक्षा की मुख्य ज़रूरत क्यों होती है? a) इंटरनेट स्पीड बढ़ाने के लिए b) सूचना संपत्तियों की रक्षा करने और व्यापार निरंतरता सुनिश्चित करने के लिए c) कर्मचारियों की संख्या कम करने के लिए d) एन्क्रिप्शन से बचने के लिए
14.	Which of the following industries is MOST dependent on cybersecurity due to sensitive data? a) Banking and Finance b) Agriculture c) Sports d) Tourism	14.	संवेदनशील डेटा की वजह से निम्नलिखित में से कौन-सा उद्योग साइबर सुरक्षा पर सबसे अधिक निर्भर है? a) Banking and Finance b) Agriculture c) Sports d) Tourism
15.	Which of the following is an example of two-factor authentication? A. Just a password B. A username and password C. Password and OTP sent to mobile D. Accessing via incognito mode	15.	निम्न में से दो-चरणीय प्रमाणीकरण (Two-Factor Authentication) का उदाहरण क्या है? A. केवल पासवर्ड B. उपयोगकर्ता नाम और पासवर्ड C. पासवर्ड और मोबाइल पर भेजा गया OTP D. इनकॉग्निटो मोड में एक्सेस करना

16.	The key length in the DES (Data Encryption Standard) cipher is: a) 56 bits b) 64 bits c) 128 bits d) 256 bits	16.	DES (डेटा एन्क्रिप्शन स्टैंडर्ड) सिफर में कुंजी (Key) की लंबाई कितनी होती है? a) 56 bits b) 64 bits c) 128 bits d) 256 bits
17.	Cybersecurity helps in maintaining the CIA triad in business. The "C" stands for: a) Communication b) Confidentiality c) Compliance d) Control	17.	साइबर सुरक्षा व्यवसाय में CIA त्रिकोण बनाए रखने में मदद करती है। यहाँ "C" का क्या मतलब है? a) Communication (संचार) b) Confidentiality (गोपनीयता) c) Compliance (अनुपालन) d) Control (नियंत्रण)
18.	The main purpose of cyber security is to protect: A. Internet speed B. Fonts and colors C. Systems, networks, and data from attacks D. Game settings	18.	साइबर सुरक्षा का मुख्य उद्देश्य क्या है? A. इंटरनेट स्पीड B. फॉन्ट्स और कलर C. सिस्टम, नेटवर्क और डेटा को हमलों से बचाना D. गेम सेटिंग्स
19.	Which of the following is NOT a component of cyber security? A. Network Security B. Application Security C. Data Backup D. Photo Editing	19.	निम्नलिखित में से कौन साइबर सुरक्षा का घटक नहीं है? A. नेटवर्क सुरक्षा B. एप्लिकेशन सुरक्षा C. डेटा बैकअप D. फोटो एडिटिंग
20.	What is cybercrime? ………… [a] A form of virtual reality gaming [b] Illegal activities conducted over the internet [c] A type of computer hardware [d] Online etiquette guidelines	20.	साइबर क्राइम क्या है? [a] वर्चुअल रियलिटी गेमिंग का एक रूप [b] इंटरनेट के माध्यम से की जाने वाली अवैध गतिविधियाँ [c] कंप्यूटर हार्डवेयर का एक प्रकार [d] ऑनलाइन शिष्टाचार के दिशा-निर्देश

21.	RSA is an example of: a) Symmetric cipher b) Asymmetric cipher c) Block cipher d) Transposition cipher	21.	RSA किसका उदाहरण है? a) Symmetric cipher b) Asymmetric cipher c) Block cipher d) Transposition cipher
22.	What does "Malware" stand for? A. Manual alert software B. Malicious Software C. Managed hardware D. Mobile aware system	22.	"मालवेयर" का पूरा रूप क्या है? A. मैनुअल अलर्ट सॉफ़्टवेयर B. मैलिशियस सॉफ़्टवेयर C. मैनेज्ड हार्डवेयर D. मोबाइल-अवेयर सिस्टम
23.	The primary goal of cyber law .... [a] To prevent all forms of online communication [b] To regulate social media usage [c] To establish legal guidelines for internet-related activities [d] To promote online anonymity	23.	साइबर क़ानून का मुख्य उद्देश्य क्या है? [a] सभी प्रकार के ऑनलाइन संचार को रोकना [b] सोशल मीडिया उपयोग को नियंत्रित करना [c] इंटरनेट से संबंधित गतिविधियों के लिए कानूनी दिशानिर्देश स्थापित करना [d] ऑनलाइन गुमनामी (Anonymity) को बढ़ावा देना
24.	Type of cybercrime involves unauthorized access to computer systems or networks with the intent to steal, alter, or destroy data .... [a] Cyberbullying [b] Hacking [c] Online fraud [d] Phishing	24.	किस प्रकार का साइबर क्राइम में बिना अनुमति कंप्यूटर सिस्टम या नेटवर्क तक पहुँचकर डेटा चुराना, बदलना या नष्ट करना शामिल है? [a] Cyberbullying (साइबर बुलिंग) [b] Hacking (हैकिंग) [c] Online fraud (ऑनलाइन धोखाधड़ी) [d] Phishing (फ़िशिंग)
25.	Which of the following is NOT a primary component of information security? a) Confidentiality b) Integrity c) Availability d) Profitability	25.	सूचना सुरक्षा का निम्नलिखित में से कौन-सा मुख्य घटक नहीं है? a) Confidentiality (गोपनीयता) b) Integrity (अखंडता) c) Availability (उपलब्धता) d) Profitability (लाभप्रदता)

26.	**What is cryptanalysis?** **A. The process of writing code** **B. The study of solving or breaking cryptographic systems** **C. The process of storing data securely** **D. The act of sending encrypted messages**	**26.**	**क्रिप्टएनालिसिस क्या है?** **A. कोड लिखने की प्रक्रिया** **B. क्रिप्टोग्राफिक सिस्टम को हल करने या तोड़ने का अध्ययन** **C. डेटा को सुरक्षित रूप से संग्रहित करने की प्रक्रिया** **D. एन्क्रिप्टेड संदेश भेजने की क्रिया**
27.	**In cryptography, a cipher is:** **a) A type of computer virus** **b) An algorithm used for encryption and decryption** **c) A firewall security rule** **d) A password storage system**	**27.**	**क्रिप्टोग्राफी में, सिफर क्या होता है?** **a) कंप्यूटर वायरस का एक प्रकार** **b) एन्क्रिप्शन और डीक्रिप्शन के लिए इस्तेमाल किया जाने वाला एल्गोरिद्म** **c) फ़ायरवॉल सुरक्षा नियम** **d) पासवर्ड स्टोरेज सिस्टम**
28.	**The term for cybercrimes that target critical infrastructure systems, such as power grids, water supplies, or transportation networks? ……….** **[a] Cyberbullying** **[b] Cyberterrorism** **[c] Online fraud** **[d] Phishing**	**28.**	**ऐसे साइबरक्राइम का क्या नाम है जो बिजली, पानी या परिवहन नेटवर्क जैसी महत्वपूर्ण अवसंरचना को निशाना बनाते हैं?** **[a] Cyberbullying (साइबर बुलिंग)** **[b] Cyberterrorism (साइबर आतंकवाद)** **[c] Online fraud (ऑनलाइन धोखाधड़ी)** **[d] Phishing (फ़िशिंग)**
29.	**Which government agency is responsible for enforcing the provisions of the IT Act 2000 and its amendments in India? ………** **[a]Ministry of Finance** **[b]Ministry of Health and Family Welfare** **[c]Ministry of Electronics and Information Technology** **[d]Ministry of Education**	**29.**	**भारत में IT Act 2000 और उसके संशोधनों को लागू करने के लिए कौन-सा सरकारी एजेंसी जिम्मेदार है?** **[a] Ministry of Finance (वित्त मंत्रालय)** **[b] Ministry of Health and Family Welfare (स्वास्थ्य और परिवार कल्याण मंत्रालय)** **[c] Ministry of Electronics and Information Technology (इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय)** **[d] Ministry of Education (शिक्षा मंत्रालय)**

30.	What is a "hashtag" used for in social media? .... [a] To separate paragraphs [b] To mark the beginning of a post [c] To categorize and link content [d] To hide content from certain users	30.	सोशल मीडिया में "हैशटैग" किस लिए इस्तेमाल किया जाता है? [a] पैराग्राफ़ को अलग करने के लिए [b] पोस्ट की शुरुआत दिखाने के लिए [c] सामग्री को वर्गीकृत और लिंक करने के लिए [d] कुछ उपयोगकर्ताओं से सामग्री छुपाने के लिए
31.	Which of these is NOT involved in the CIA Triad? a) Confidentiality c)Integrity b) Availability d Authenticity	31.	इनमें से कौन CIA Triad का हिस्सा नहीं है? a) Confidentiality (गोपनीयता) b) Availability (उपलब्धता) c) Integrity (अखंडता) d) Authenticity (प्रामाणिकता)
32.	Which of these is not covered under cyber law? A. Online fraud B. Intellectual property rights C. Cyberbullying D. Traffic signals	32.	निम्न में से कौन साइबर कानून के अंतर्गत नहीं आता है? A. ऑनलाइन धोखाधड़ी B. बौद्धिक संपदा अधिकार C. साइबरबुलिंग D. ट्रैफिक सिग्नल
33.	Which Indian agency investigates cybercrimes? A. RBI B. TRAI C. CERT-In D. ISRO	33.	भारत में कौन-सी एजेंसी साइबर अपराधों की जांच करती है? A. RBI B. TRAI C. CERT-In D. ISRO
34.	Which of the following is a human (people) component of information security? a) Firewalls b) Intrusion detection system c) Employee awareness training d) Antivirus software	34.	सूचना सुरक्षा का मानव (मानव-संबंधी) घटक निम्न में से कौन सा है? a) फ़ायरवॉल b) घुसपैठ पता लगाने की प्रणाली c) कर्मचारी जागरूकता प्रशिक्षण d) एंटीवायरस सॉफ़्टवेयर
35.	Which of the following is not a punishment under cyber law? A. Fine B. Imprisonment C. Warning letter D. Both A and B	35.	निम्न में से कौन साइबर कानून के अंतर्गत सजा नहीं है? A. जुर्माना B. कारावास C. चेतावनी पत्र D. उपरोक्त A और B दोनों

36.	Which operation is commonly used in OTP encryption and decryption? a) XOR (Exclusive OR) b) Addition modulo 10 only c) Hashing d) RSA exponentiation	36.	OTP (One-Time Pad) एन्क्रिप्शन और डीक्रिप्शन में आमतौर पर कौन सा ऑपरेशन इस्तेमाल होता है? a) XOR (Exclusive OR) b) Addition modulo 10 only c) Hashing d) RSA exponentiation
37.	A patent holder can prevent others from: A. Selling their invention B. Copying their invention without permission C. Using their invention D. All of the above	37.	पेटेंट धारक दूसरों को किससे रोक सकता है? A. उनके आविष्कार को बेचने से B. उनके आविष्कार की नकल करने से C. उनके आविष्कार का उपयोग करने से D. उपरोक्त सभी
38.	What is the main purpose of developing an information system (IS)? a) To store physical files b) To support decision-making and business processes c) To increase hardware costs d) To reduce internet speed	38.	सूचना प्रणाली (Information System) विकसित करने का मुख्य उद्देश्य क्या है? a) भौतिक फ़ाइलें संग्रहित करना b) निर्णय लेने और व्यापार प्रक्रियाओं का समर्थन करना c) हार्डवेयर लागत बढ़ाना d) इंटरनेट स्पीड कम करना
39.	Security attacks are broadly classified into: a) Internal and External attacks b) Active and Passive attacks c) Physical and Logical attacks d) All of the above	39.	सुरक्षा हमलों (Security Attacks) को व्यापक रूप से किस प्रकार वर्गीकृत किया जाता है? a) आंतरिक और बाहरी हमले b) सक्रिय और निष्क्रिय हमले c) भौतिक और तार्किक हमले d) उपरोक्त सभी)
40.	Digital law refers to: A. Laws regarding physical crime B. Laws related to internet, data protection, and online activities C. Laws related to land ownership D. Laws about banking only	40.	डिजिटल कानून का क्या अर्थ है? A. भौतिक अपराधों से संबंधित कानून B. इंटरनेट, डेटा सुरक्षा और ऑनलाइन गतिविधियों से संबंधित कानून C. भूमि स्वामित्व से संबंधित कानून D. केवल बैंकिंग से संबंधित कानून

41.	Which of the following is not covered by Digital Law? A. Online fraud B. Copyright infringement in digital media C. Privacy of digital users D. Traffic laws for vehicles	41.	निम्न में से कौन डिजिटल कानून के अंतर्गत नहीं आता है? A. ऑनलाइन धोखाधड़ी B. डिजिटल मीडिया में कॉपीराइट उल्लंघन C. डिजिटल उपयोगकर्ताओं की गोपनीयता D. वाहनों के लिए ट्रैफिक कानून
42.	The Information Technology Act (ITA) 2000 of India addresses: A. Digital marketing B. Online privacy and security C. Digital media advertising D. Internet censorship	42.	भारत का सूचना प्रौद्योगिकी अधिनियम (आईटी अधिनियम) 2000 किससे संबंधित है? A. डिजिटल मार्केटिंग B. ऑनलाइन गोपनीयता और सुरक्षा C. डिजिटल मीडिया विज्ञापन D. इंटरनेट सेंसरशिप
43.	Digital signatures are used to: A. Ensure the physical security of a document B. Authenticate digital communications and documents C. Secure online banking transactions only D. Provide free access to digital content	43.	डिजिटल हस्ताक्षर का उपयोग किया जाता है: A. किसी दस्तावेज़ की भौतिक सुरक्षा सुनिश्चित करने के लिए B. डिजिटल संचार और दस्तावेजों को प्रमाणित करने के लिए C. केवल ऑनलाइन बैंकिंग लेनदेन को सुरक्षित करने के लिए D. डिजिटल सामग्री तक मुफ्त पहुँच देने के लिए
44.	Copyright protects: A. Physical property B. Inventions C. Original works of authorship D. Business names	44.	कॉपीराइट किसकी सुरक्षा करता है? A. भौतिक संपत्ति B. आविष्कारों C. मौलिक साहित्यिक या कलात्मक कृतियाँ D. व्यापार नाम
45.	Which of the following is NOT protected by copyright? A. Books B. Songs C. Ideas D. Movies	45.	निम्न में से कौन-सा कॉपीराइट द्वारा संरक्षित नहीं है? A. पुस्तकें B. गीत C. विचार D. फिल्में

46.	The symbol © represents: A. A company B. Copy service C. Copyright D. Commercial use	46.	प्रतीक © का अर्थ है: A. एक कंपनी B. कॉपी सेवा C. कॉपीराइट D. व्यावसायिक उपयोग
47.	Copyright law grants the author exclusive rights to: A. Use, distribute, and reproduce their work B. Create physical copies only C. Open a business D. Protect inventions	47.	कॉपीराइट कानून लेखक को क्या अधिकार देता है? A. अपने कार्य का उपयोग, वितरण और पुनरुत्पादन करने का B. केवल भौतिक प्रतियाँ बनाने का C. एक व्यवसाय खोलने का D. आविष्कारों की सुरक्षा करने का
48.	Which of the following is NOT an aspect of information security? a) Confidentiality b) Integrity c) Availability d) Entertainment	48.	सूचना सुरक्षा का निम्नलिखित में से कौन सा पहलू नहीं है? a) गोपनीयता b) अखंडता c) उपलब्धता d) मनोरंजन
49.	SQL Injection attacks target: a) Database systems b) Physical network devices c) User passwords only d) Email servers	49.	SQL Injection हमले किसको निशाना बनाते हैं? a) डेटाबेस सिस्टम्स b) भौतिक नेटवर्क डिवाइस c) केवल उपयोगकर्ता पासवर्ड d) ईमेल सर्वर
50.	Ethical hacking is: a) Hacking without permission b) Unauthorized access to steal data c) Authorized attempts to find and fix security vulnerabilities d) Installing malware on a system	50.	एथिकल हैकिंग क्या है? a) अनुमति के बिना हैकिंग करना b) डेटा चुराने के लिए अनधिकृत पहुँच c) सुरक्षा कमजोरियों को खोजने और ठीक करने के लिए अधिकृत प्रयास d) सिस्टम में मैलवेयर इंस्टॉल करना

51.	Which component of information security ensures that data is not altered or tampered with? A) Availability B) Integrity C) Authentication D) Confidentiality	51.	सूचना सुरक्षा का कौन-सा घटक यह सुनिश्चित करता है कि डेटा में कोई बदलाव या छेड़छाड़ न हो? A. उपलब्धता B. अखंडता (Integrity) C. प्रमाणीकरण D. गोपनीयता
52.	Which of the following is an example of a physical security control? A) Using strong passwords B) Encrypting data C) Installing security cameras D) Running anti-virus software	52.	निम्नलिखित में से कौन-सा भौतिक सुरक्षा नियंत्रण (Physical Security Control) का उदाहरण है? A. मजबूत पासवर्ड का उपयोग करना B. डेटा को एन्क्रिप्ट करना C. सुरक्षा कैमरे लगाना D. एंटीवायरस सॉफ़्टवेयर चलाना
53.	Which of the following is a preventive security technique? a) Firewall b) IDS (Intrusion Detection System) c) Logging d) Hash verification	53.	निम्न में से कौन-सा सुरक्षा तकनीक रोकथाम (Preventive) के लिए है? a) फ़ायरवॉल b) IDS (घुसपैठ पहचान प्रणाली) c) लॉगिंग d) हैश सत्यापन
54.	Which of the following is considered unethical behavior in information security? a) Reporting a discovered vulnerability to the organization b) Accessing confidential data without authorization c) Encrypting sensitive data for protection d) Following company security policies	54.	सूचना सुरक्षा में निम्नलिखित में से कौन सा अनैतिक व्यवहार माना जाता है? a) खोजी गई vulnerability को संगठन को रिपोर्ट करना b) अनधिकृत रूप से गोपनीय डेटा तक पहुंच प्राप्त करना c) संवेदनशील डेटा को सुरक्षा के लिए एन्क्रिप्ट करना d) कंपनी की सुरक्षा नीतियों का पालन करना
55.	Social engineering attacks exploit: a) Weak software b) Human psychology and trust c) Network protocols only d) Encryption algorithms	55.	सोशल इंजीनियरिंग हमले किसका फायदा उठाते हैं? a) कमजोर सॉफ़्टवेयर b) मानव मनोविज्ञान और विश्वास c) केवल नेटवर्क प्रोटोकॉल d) एन्क्रिप्शन एल्गोरिदम

56.	Which document is MOST closely related to a policy review process? a) System Log File b) Compliance Audit Report c) Personal Notes of Employees d) Internet Usage History	56.	कौन सा दस्तावेज़ नीति समीक्षा (Policy Review) प्रक्रिया से सबसे अधिक संबंधित है? a) सिस्टम लॉग फ़ाइल b) अनुपालन ऑडिट रिपोर्ट c) कर्मचारियों के व्यक्तिगत नोट्स d) इंटरनेट उपयोग का इतिहास
57.	A user who violates a software license agreement can face: A. Software updates B. Rewards C. Legal action or penalties D. Bonus features	57.	यदि कोई उपयोगकर्ता सॉफ़्टवेयर लाइसेंस समझौते का उल्लंघन करता है तो उसे क्या सामना करना पड़ सकता है? A. सॉफ़्टवेयर अपडेट B. पुरस्कार C. कानूनी कार्रवाई या दंड D. बोनस फ़ीचर्स
58.	Unauthorized copying of software or data is a violation of: a) Confidentiality b) Intellectual property rights c) Availability d) Integrity	58.	सॉफ़्टवेयर या डेटा की अनधिकृत नकल किसका उल्लंघन है? a) Confidentiality (गोपनीयता) b) Intellectual property rights (बौद्धिक संपदा अधिकार) c) Availability (उपलब्धता) d) Integrity (अखंडता)
59.	Cybersecurity professionals must maintain: a) Ethical behavior, professional standards, and compliance with laws b) Only technical skills c) Network speed optimization d) Only physical security	59.	साइबर सुरक्षा पेशेवरों को क्या बनाए रखना चाहिए? a) Ethical behavior, professional standards, and compliance with laws b) केवल तकनीकी कौशल c) नेटवर्क गति अनुकूलन d) केवल भौतिक सुरक्षा
60.	Which type of email is considered a threat in email security? A. Welcome email from HR B. Email with an unknown link or attachment C. Monthly newsletter D. Internal team update	60.	निम्न में से कौन-सी ईमेल ईमेल सुरक्षा के लिए खतरा मानी जाती है? A. एचआर से स्वागत ईमेल B. अज्ञात लिंक या अटैचमेंट वाली ईमेल C. मासिक न्यूज़लेटर D. आंतरिक टीम अपडेट

61.	One way to prevent phishing attacks is: A. Always reply to unknown emails B. Click on flashy banners C. Use spam filters and verify senders D. Never read emails	61.	फिशिंग हमलों को रोकने का एक तरीका है: A. अज्ञात ईमेल का हमेशा जवाब देना B. चमकदार बैनर पर क्लिक करना C. स्पैम फ़िल्टर का उपयोग करना और प्रेषक को सत्यापित करना D. कभी भी ईमेल न पढ़ना
62.	Intrusion Detection Systems (IDS) are used to: a) Encrypt data b) Monitor network traffic and detect suspicious activity c) Backup files d) Control user access	62.	Intrusion Detection System (IDS) किस लिए उपयोग किया जाता है? a) डेटा एन्क्रिप्ट करना b) नेटवर्क ट्रैफ़िक की निगरानी करना और संदिग्ध गतिविधि का पता लगाना c) फाइलों का बैकअप लेना d) उपयोगकर्ता की पहुँच को नियंत्रित करना
63.	A substitution cipher works by: A. Rearranging letters in a message B. Replacing each letter with another letter C. Hiding the message in an image D. Encrypting numbers only	63.	एक सब्सटीट्यूशन सिफर काम करता है: A. संदेश के अक्षरों को पुनर्व्यवस्थित करके B. प्रत्येक अक्षर को किसी अन्य अक्षर से बदलकर C. संदेश को किसी चित्र में छुपाकर D. केवल संख्याओं को एन्क्रिप्ट करके
64.	The main weakness of substitution ciphers is that they can be broken by: a) Frequency analysis b) Brute-force only c) Reverse engineering d) Quantum computing	64.	Substitution cipher की मुख्य कमजोरी यह है कि इसे किसके द्वारा तोड़ा जा सकता है? a) आवृत्ति विश्लेषण b) केवल ब्रूट-फोर्स c) रिवर्स इंजीनियरिंग d) क्वांटम कंप्यूटिंग
65.	In a monoalphabetic cipher, each letter of the plaintext: A. Maps to itself B. Maps to a different letter based on a fixed substitution C. Is reversed D. Is doubled	65.	मोनो-अल्फाबेटिक सिफर में, प्लेनटेक्स्ट के प्रत्येक अक्षर का: A. अपने आप से मिलान होता है B. एक निश्चित प्रतिस्थापन के आधार पर किसी अन्य अक्षर से मिलान होता है C. उल्टा किया जाता है D. दोहराया जाता है

66.	Which cipher uses a pair of public and private keys? a) Stream cipher b) Block cipher c) Symmetric cipher d) Asymmetric cipher	66.	कौन सा सिफर सार्वजनिक और निजी कुंजी के जोड़े का उपयोग करता है? a) स्ट्रीम सिफर b) ब्लॉक सिफर c) समान कुंजी सिफर d) असमान कुंजी सिफर
67.	What does X.800 define? A. Encryption algorithms B. Security services and mechanisms C. Network topologies D. Firewall configurations	67.	X.800 क्या परिभाषित करता है? A. एन्क्रिप्शन एल्गोरिदम B. सुरक्षा सेवाएं और तंत्र C. नेटवर्क टोपोलॉजी D. फ़ायरवॉल कॉन्फ़िगरेशन
68.	How often should information security policies ideally be reviewed? a) Once every 10 years b) Only when a breach occurs c) Periodically (e.g., annually or semi-annually) d) Never, once created they are permanent	68.	सूचना सुरक्षा नीतियों की आदर्श रूप से कितनी बार समीक्षा की जानी चाहिए? a) हर 10 साल में एक बार b) केवल जब कोई सुरक्षा उल्लंघन हो c) नियमित अंतराल पर (जैसे, सालाना या अर्धवार्षिक) d) कभी नहीं, एक बार बन जाने के बाद स्थायी होती हैं
69.	One-way hash functions are mostly used for: A. Sending videos B. File compression C. Password storage and data integrity D. Encrypting emails	69.	वन-वे हैश फ़ंक्शन का अधिकांश उपयोग होता है: A. वीडियो भेजने के लिए B. फाइल कंप्रेशन के लिए C. पासवर्ड स्टोरेज और डेटा अखंडता के लिए D. ईमेल एन्क्रिप्शन के लिए
70.	A one-way hash function is also known as: A. Symmetric encryption B. Hash algorithm C. Biometric matcher D. Reversible cipher	70.	एक वन-वे हैश फ़ंक्शन को क्या कहा जाता है? A. सममित एन्क्रिप्शन B. हैश एल्गोरिदम C. बायोमेट्रिक मैचर D. रिवर्सिबल सिफर

71.	**Which of the following is a basic type of cryptography?** **A. Block chaining** **B. Hashing** **C. Symmetric key cryptography** **D. Packet sniffing**	71.	**निम्नलिखित में से कौन-सा क्रिप्टोग्राफी का मूल प्रकार है?** **A. ब्लॉक चेनिंग** **B. हैशिंग** **C. सममित कुंजी क्रिप्टोग्राफी** **D. पैकेट स्निफिंग**
72.	**In symmetric cryptography, the same key is used for:** **A. Decryption only** **B. Encryption and decryption** **C. Only hashing** **D. Creating digital signatures**	72.	**सममित क्रिप्टोग्राफी में एक ही कुंजी का उपयोग किया जाता है:** **A. केवल डिक्रिप्शन के लिए** **B. एन्क्रिप्शन और डिक्रिप्शन दोनों के लिए** **C. केवल हैशिंग के लिए** **D. डिजिटल हस्ताक्षर बनाने के लिए**
73.	**Public key cryptography uses:** **A. One key for both parties** **B. The same key for all users** **C. A pair of keys (public and private)** **D. No keys**	73.	**सार्वजनिक कुंजी क्रिप्टोग्राफी में उपयोग किया जाता है:** **A. दोनों पक्षों के लिए एक ही कुंजी** **B. सभी उपयोगकर्ताओं के लिए एक ही कुंजी** **C. कुंजियों की एक जोड़ी (पब्लिक और प्राइवेट)** **D. कोई कुंजी नहीं**
74.	**Which algorithm is used in asymmetric cryptography?** **A. AES** **B. RSA** **C. DES** **D. MD5**	74.	**असममित क्रिप्टोग्राफी में कौन-सा एल्गोरिदम उपयोग किया जाता है?** **A. AES** **B. RSA** **C. DES** **D. MD5**
75.	**What is plaintext?** **A. Encrypted message** **B. A random code** **C. Original, readable message before encryption** **D. Compressed data**	75.	**प्लेनटेक्स्ट क्या होता है?** **A. एन्क्रिप्टेड संदेश** **B. एक रैंडम कोड** **C. एन्क्रिप्शन से पहले का मूल, पढ़ने योग्य संदेश** **D. संकुचित डाटा**
76.	**In substitution ciphers, the frequency distribution of letters in the ciphertext is:** **a) Same as plaintext but disguised** **b) Completely changed** **c) Random and unrelated** **d) Always equal**	76.	**Substitution cipher में ciphertext में अक्षरों का आवृत्ति वितरण (frequency distribution) कैसा होता है?** **a) Plaintext के समान लेकिन छिपा हुआ** **b) पूरी तरह बदल गया** **c) यादृच्छिक और असंबंधित** **d) हमेशा समान**

77.	The process of converting ciphertext back to plaintext is called: A. Transferring B. Encoding C. Decryption D. Re-coding	77.	सिफरटेक्स्ट को वापस प्लेनटेक्स्ट में बदलने की प्रक्रिया को क्या कहते हैं? A. ट्रांसफरिंग B. एन्कोडिंग C. डिक्रिप्शन D. री-कोडिंग
78.	What is used to lock and unlock messages in cryptography? A. Mouse B. Monitor C. Key D. Folder	78.	क्रिप्टोग्राफी में संदेश को लॉक और अनलॉक करने के लिए क्या उपयोग होता है? A. माउस B. मॉनिटर C. कुंजी (Key) D. फोल्डर
79.	Which statement is TRUE about transposition ciphers? a) They change the letters into different letters b) They preserve the letter frequencies of plaintext c) They cannot be combined with substitution d) They destroy the order of the alphabet completely	79.	Transposition cipher के बारे में कौन सा कथन सही है? a) वे अक्षरों को अलग अक्षरों में बदल देते हैं b) वे plaintext के अक्षरों की आवृत्ति संरक्षित रखते हैं c) उन्हें substitution के साथ जोड़ा नहीं जा सकता d) वे पूरी तरह से अक्षरों के क्रम को नष्ट कर देते हैं
80.	The public key is shared with: A. No one B. Only the boss C. Everyone D. Only with your compute	80.	सार्वजनिक कुंजी किसके साथ साझा की जाती है? A. किसी के साथ नहीं B. केवल बॉस के साथ C. सभी के साथ D. केवल अपने कंप्यूटर के साथ
81.	If plaintext bit = 1 and key bit = 0, the XOR ciphertext bit will be: a) 0 b) 1 c) Random d) Same as key	81.	यदि plaintext bit = 1 और key bit = 0 है, तो XOR ciphertext bit क्या होगा? a) 0 b) 1 c) Random (यादृच्छिक) d) Same as key (कुंजी के समान)

82.	**Which of the following is a real use of cryptography?** **A.** Sending secret messages **B. Making sandwiches** **C. Watching movies** **D. Charging phones**	**82.**	**निम्नलिखित में से क्रिप्टोग्राफी का असली उपयोग क्या है?** **A. गुप्त संदेश भेजना** **B. सैंडविच बनाना** **C. फिल्में देखना** **D. फोन चार्ज करना**
83.	**Which one is more secure – symmetric or asymmetric encryption?** **A. Symmetric** **B.** Asymmetric **C. None** **D. Both are unsafe**	**83.**	**कौन-सी अधिक सुरक्षित है – सममित या असममित एन्क्रिप्शन?** **A. सममित** **B. असममित** **C. कोई नहीं** **D. दोनों असुरक्षित हैं**
84.	**What does a website's privacy policy usually explain?** **A) How to improve your internet speed** **B)** How the website collects and uses your data **C) The price of internet services** **D) How to create a new website**	**84.**	**किसी वेबसाइट की गोपनीयता नीति (Privacy Policy) आमतौर पर क्या बताती है?** **A. अपनी इंटरनेट स्पीड कैसे बढ़ाएँ** **B. वेबसाइट आपका डेटा कैसे एकत्रित और उपयोग करती है** **C. इंटरनेट सेवाओं की कीमत** **D. नई वेबसाइट कैसे बनाएँ**
85.	**XOR cipher is considered weak because:** **a) It is irreversible** **b)** If the key is short or reused, patterns can be detected **c) It increases data size** **d) It requires large key storage**	**85.**	**XOR cipher को कमजोर क्यों माना जाता है?** **a) यह अप्रतिवर्तनीय है** **b) यदि key छोटी हो या पुन: उपयोग की जाए, तो पैटर्न पता लगाया जा सकता है** **c) यह डेटा आकार बढ़ाता है** **d) इसके लिए बड़ी कुंजी संग्रहण की आवश्यकता होती है**
86.	**XOR is mainly used in cryptography because it is:** **a) Complex and slow** **b)** Simple, fast, and reversible **c) Always random** **d) Requires no key**	**86.**	**XOR का क्रिप्टोग्राफी में मुख्य उपयोग क्यों है?** **a) जटिल और धीमा** **b) सरल, तेज़ और प्रतिवर्तनीय** **c) हमेशा यादृच्छिक** **d) इसके लिए कोई key आवश्यक नहीं**

87.	Which of the following is a key objective of security policies? a) Protect information assets b) Define responsibilities of users c) Establish procedures for incident response d) All of the above	87.	सुरक्षा नीतियों का प्रमुख उद्देश्य क्या है? a) सूचना संपत्तियों की सुरक्षा करना (Protect information assets) b) उपयोगकर्ताओं की जिम्मेदारियों को परिभाषित करना (Define responsibilities of users) c) घटना प्रतिक्रिया के लिए प्रक्रियाएँ स्थापित करना (Establish procedures for incident response) d) उपरोक्त सभी (All of the above)
88.	Which part of the CIA Triad ensures that data is kept accurate and free from tampering? A) Confidentiality B) Integrity C) Availability D) Authentication	88.	CIA ट्रायड का कौन-सा भाग डेटा की सटीकता और छेड़छाड़ से सुरक्षा सुनिश्चित करता है? A. गोपनीयता B. अखंडता (Integrity) C. उपलब्धता D. प्रमाणीकरण
89.	The "A" in the CIA Triad stands for: A) Authentication B) Access C) Availability D) Authorization	89.	CIA ट्रायड में "A" का मतलब क्या होता है? A. प्रमाणीकरण B. एक्सेस C. उपलब्धता (Availability) D. अधिकृत करना
90.	What is the main goal of information security? A) To provide entertainment to users B) To ensure confidentiality, integrity, and availability of data C) To increase website traffic D) To track user activities	90.	सूचना सुरक्षा का मुख्य उद्देश्य क्या है? A. उपयोगकर्ताओं को मनोरंजन प्रदान करना B. डेटा की गोपनीयता, अखंडता और उपलब्धता सुनिश्चित करना C. वेबसाइट ट्रैफिक बढ़ाना D. उपयोगकर्ता गतिविधियों को ट्रैक करना
91.	The main purpose of a security policy review process is to: a) Delete old policies permanently b) Ensure policies remain current, effective, and aligned with business goals c) Replace security with compliance documents d) Train only new employees	91.	सुरक्षा नीति समीक्षा प्रक्रिया का मुख्य उद्देश्य क्या है? a) पुरानी नीतियों को स्थायी रूप से हटाना b) सुनिश्चित करना कि नीतियाँ वर्तमान, प्रभावी और व्यावसायिक लक्ष्यों के अनुरूप बनी रहें c) सुरक्षा दस्तावेज़ों को केवल अनुपालन दस्तावेज़ों से बदलना d) केवल नए कर्मचारियों को प्रशिक्षण देना

92.	What is a firewall used for in information security? A) To speed up internet access B) To protect against unauthorized access to a network C) To store data in the cloud D) To create stronger passwords	92.	सूचना सुरक्षा में फ़ायरवॉल का उपयोग किसलिए किया जाता है? A. इंटरनेट एक्सेस तेज करने के लिए B. नेटवर्क में अनधिकृत एक्सेस से बचाने के लिए C. डेटा को क्लाउड में स्टोर करने के लिए D. मजबूत पासवर्ड बनाने के लिए
93.	Which of the following helps secure online accounts? A) Using weak passwords B) Enabling multi-factor authentication C) Ignoring software updates D) Sharing passwords with others	93.	ऑनलाइन अकाउंट को सुरक्षित रखने में कौन मदद करता है? A. कमजोर पासवर्ड का उपयोग B. मल्टी-फैक्टर ऑथेंटिकेशन सक्षम करना C. सॉफ़्टवेयर अपडेट को अनदेखा करना D. पासवर्ड दूसरों के साथ साझा करना
94.	Which of the following is an example of authentication in information security? A) Encrypting data B) Verifying a user's identity through a password C) Storing data securely D) Making backups of data	94.	सूचना सुरक्षा में प्रमाणीकरण (Authentication) का उदाहरण क्या है? A. डेटा एन्क्रिप्ट करना B. पासवर्ड के जरिए उपयोगकर्ता की पहचान की पुष्टि करना C. डेटा को सुरक्षित रूप से स्टोर करना D. डेटा की बैकअप कॉपी बनाना
95.	Which of the following helps ensure data integrity? A) Making backups of files B) Encrypting data C) Using checksums to verify data has not changed D) Installing firewalls	95.	डेटा की अखंडता सुनिश्चित करने में क्या मदद करता है? A. फ़ाइलों का बैकअप बनाना B. डेटा को एन्क्रिप्ट करना C. चेकसम का उपयोग करके यह जांचना कि डेटा बदला नहीं है D. फ़ायरवॉल इंस्टॉल करना
96.	A transposition cipher works by: a) Substituting each letter with another letter b) Shuffling/rearranging the order of characters without changing them c) Converting text to binary d) Adding numbers to letters	96.	Transposition cipher कैसे काम करता है? a) प्रत्येक अक्षर को दूसरे अक्षर से बदलना (Substituting each letter with another letter) b) अक्षरों को बदलने के बिना क्रम को फेरबदल / पुनर्व्यवस्थित करना c) टेक्स्ट को बाइनरी में बदलना (Converting text to binary) d) अक्षरों में संख्याएँ जोड़ना (Adding numbers to letters)

97.	Identity theft in cybercrime refers to: a) Stealing personal information to commit fraud b) Deleting unwanted emails c) Installing antivirus software d) Changing passwords for security	97.	साइबर क्राइम में Identity theft का क्या मतलब है? a) धोखाधड़ी करने के लिए व्यक्तिगत जानकारी चुराना b) अनचाहे ईमेल हटाना c) एंटीवायरस सॉफ़्टवेयर इंस्टॉल करना d) सुरक्षा के लिए पासवर्ड बदलना
98.	Which law in India deals with cybercrime and electronic commerce? a) Indian Penal Code (IPC) only b) Information Technology Act, 2000 c) Companies Act d) Cybersecurity Act 2020	98.	भारत में कौन सा कानून साइबरक्राइम और इलेक्ट्रॉनिक कॉमर्स से संबंधित है? a) केवल Indian Penal Code (IPC) b) Information Technology Act, 2000 c) Companies Act d) Cybersecurity Act 2020
99.	Which of the following is a preventive measure against cybercrime? a) Using strong passwords b) Avoiding software updates c) Sharing passwords openly d) Disabling antivirus	99.	निम्न में से कौन सा साइबरक्राइम के खिलाफ रोकथाम उपाय है? a) मजबूत पासवर्ड का उपयोग b) सॉफ़्टवेयर अपडेट से बचना c) पासवर्ड को खुले में साझा करना d) एंटीवायरस को डिसेबल करना
100.	Which of the following is an example of cybercrime? a) Hacking into a bank account b) Driving without a license c) Stealing physical money d) Shoplifting	100.	निम्न में से कौन सा साइबरक्राइम का उदाहरण है? a) बैंक अकाउंट में हैकिंग b) बिना लाइसेंस ड्राइव करना c) भौतिक पैसे की चोरी d) चोरी करना

Rough Work / रफ कार्य

Example :

Question :

Q.1 Ⓐ ● Ⓒ Ⓓ

Q.2 Ⓐ Ⓑ ● Ⓓ

Q.3 Ⓐ ● Ⓒ Ⓓ

5. Each question carries equal marks. Marks will be awarded according to the number of correct answers you have.

6. All answers are to be given on OMR Answer Sheet only. Answers given anywhere other than the place specified in the answer sheet will not be considered valid.

7. Before writing anything on the OMR Answer Sheet, all the instructions given in it should be read carefully.

8. After the completion of the examination, candidates should leave the examination hall only after providing their OMR Answer Sheet to the invigilator. Candidate can carry their Question Booklet.

9. There will be no negative marking.

10. Rough work, if any, should be done on the blank pages provided for the purpose in the booklet.

11. To bring and use of log-book, calculator, pager & cellular phone in examination hall is prohibited.

12. In case of any difference found in English and Hindi version of the question, the English version of the question will be held authentic.

Impt. On opening the question booklet, first check that all the pages of the question booklet are printed properly. If there is any discrepancy in the question Booklet, then after showing it to the invigilator, get another question Booklet of the same series.

उदाहरण :

प्रश्न :

प्रश्न 1 Ⓐ ● Ⓒ Ⓓ

प्रश्न 2 Ⓐ Ⓑ ● Ⓓ

प्रश्न 3 Ⓐ ● Ⓒ Ⓓ

5. प्रत्येक प्रश्न के अंक समान हैं। आपके जितने उत्तर सही होंगे, उन्हीं के अनुसार अंक प्रदान किये जायेंगे।

6. सभी उत्तर केवल ओ०एम०आर० उत्तर-पत्रक (OMR Answer Sheet) पर ही दिये जाने हैं। उत्तर-पत्रक में निर्धारित स्थान के अलावा अन्यत्र कहीं पर दिया गया उत्तर मान्य नहीं होगा।

7. ओ०एम०आर० उत्तर-पत्रक (OMR Answer Sheet) पर कुछ भी लिखने से पूर्व उसमें दिये गये सभी अनुदेशों को सावधानीपूर्वक पढ़ लिया जाये।

8. परीक्षा समाप्ति के उपरान्त परीक्षार्थी कक्ष निरीक्षक को अपनी OMR Answer Sheet उपलब्ध कराने के बाद ही परीक्षा कक्ष से प्रस्थान करें। परीक्षार्थी अपने साथ प्रश्न-पुस्तिका ले जा सकते हैं।

9. निगेटिव मार्किंग नहीं है।

10. कोई भी रफ कार्य, प्रश्न-पुस्तिका में, रफ-कार्य के लिए दिए खाली पेज पर ही किया जाना चाहिए।

11. परीक्षा-कक्ष में लॉग-बुक, कैल्कुलेटर, पेजर तथा सेल्युलर फोन ले जाना तथा उसका उपयोग करना वर्जित है।

12. प्रश्न के हिन्दी एवं अंग्रेजी रूपान्तरण में भिन्नता होने की दशा में प्रश्न का अंग्रेजी रूपान्तरण ही मान्य होगा।

महत्वपूर्णः प्रश्नपुस्तिका खोलने पर प्रथमतः जाँच कर देख लें कि प्रश्नपुस्तिका के सभी पृष्ठ भलीभाँति छपे हुए हैं। यदि प्रश्नपुस्तिका में कोई कमी हो, तो कक्षनिरीक्षक को दिखाकर उसी सिरीज की दूसरी प्रश्नपुस्तिका प्राप्त कर लें।