Roll. No. .....

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

Question Booklet Number

BCA (SEM.-VI) (NEP) (SUPPLE.)EXAMINATION, 2024-25

COMPUTER APPLICATION

(Information & Cyber Security)

[BCA-6001]

Paper Code							
Z	0	1	0	1	2	1	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. Who are termed as netizens?
   (A) People who work in IT companies
   (B) Citizens who use the internet actively
   (C) Cyber law enforcement officers
   (D) Computer programmers
2. The Information Technology Act, 2000 was made to:
   (A) Provide legal recognition to electronic transactions
   (B) Promote software exports
   (C) Regulate telecommunication companies
   (D) Monitor social media content
3. Which section of IT Act, 2000 deals with hacking?
   (A) Section 43
   (B) Section 65
   (C) Section 72
   (D) Section 66
4. Which of the following is an example of an electronic record?
   (A) Printed invoice
   (B) Handwritten agreement
   (C) Digital contract in PDF format
   (D) Court judgment in book form
5. Which of the following is NOT a challenge of e-commerce?
   (A) Cyber fraud
   (B) Identity theft
   (C) Paper-based records
   (D) Secure payment
6. The full form of IDS is:
   (A) Internet Detection System
   (B) Intrusion Detection System
   (C) Information Defense Strategy
   (D) Integrated Defense Security
7. Which of the following best describes an IDS?
   (A) Prevents intrusion automatically
   (B) Detects malicious activity and alerts
   (C) Encrypts data for secure transmission
   (D) Creates firewalls for networks
8. Which system actively blocks unauthorized access?
   (A) IDS
   (B) PKI
   (C) IPS
   (D) Firewall only
9. PKI is used primarily for:
   (A) Digital forensics
   (B) Encryption and authentication
   (C) Ethical hacking
   (D) Intrusion prevention

10. In PKI, CA stands for:
    (A) Central Authentication
    (B) Certified Auditor
    (C) Cybersecurity Agency
    (D) Certificate Authority
11. A digital certificate is issued by:
    (A) User
    (B) Certification Authority
    (C) Government only
    (D) Network administrator
12. Which key is not shared in asymmetric cryptography?
    (A) Only private key
    (B) Only public key
    (C) Both public and private keys
    (D) Session key
13. Which of the following is NOT part of PKI?
    (A) Digital certificates
    (B) IDS
    (C) Certificate Authorities
    (D) Public/private keys
14. What is the main function of an Intrusion Prevention System?
    (A) Monitor traffic
    (B) Block malicious traffic in real time
    (C) Generate audit logs only
    (D) Encrypt data packets
15. Which of these is an example of asymmetric encryption algorithm?
    (A) MD5
    (B) RSA
    (C) DES
    (D) Blowfish
16. Which of these is used to prove authenticity and integrity of digital communication?
    (A) Proxy server
    (B) Firewall
    (C) Digital certificate
    (D) Antivirus
17. Which organization regulates cybersecurity in India under IT Act?
    (A) NASSCOM
    (B) CERT-In
    (C) TRAI
    (D) CBI
18. Cyberspace refers to:
    (A) Physical infrastructure of the internet
    (B) Virtual environment of digital communication
    (C) Social networking only
    (D) Hardware and software systems
19. Which of the following is an example of an electronic record?
    (A) Printed invoice
    (B) Handwritten agreement
    (C) Income Tax return from incometax department
    (D) Court judgment in book form
20. Which of the following is NOT a hash algorithm used in digital signature?
    (A) SHA-1
    (B) SHA 256
    (C) RSA
    (D) MD5

21. Computer security's primary goal is for:
(A) Protecting only software
(B) Protecting hardware only
(C) Protection of data, devices, and networks
(D) Protecting internet cables

22. Hacking is:
(A) Authorized penetration testing
(B) Unauthorized access to a computer system
(C) Writing a new software
(D) Blocking websites

23. Cracking refers to:
(A) Ethical hacking
(B) Breaking passwords or software protection illegally
(C) Testing applications for bugs
(D) Writing encryption codes

24. Sneaking in cybersecurity means:
(A) Entering a system undetected
(B) Monitoring network traffic
(C) Guessing passwords
(D) Sending phishing emails

25. A Trojan Horse is:
(A) A self-replicating program
(B) Malicious software disguised as useful software
(C) A denial-of-service tool
(D) A network sniffer

26. A virus is defined as:
(A) A self-replicating malicious program that needs a host
(B) A standalone malicious code that spreads automatically
(C) A hardware attack
(D) A social engineering trick

27. A logic bomb is triggered by:
(A) Opening an email
(B) Specific event or condition
(C) Antivirus scan
(D) Internet connectivity

28. Denial-of-Service (DoS) attacks primarily aim to:
(A) Destroy hardware
(B) Steal sensitive data
(C) Make a system or service unavailable
(D) Encrypt user data

29. Which attack involves redirecting traffic to a fake DNS server?
(A) IP Spoofing
(B) DNS Spoofing
(C) ARP Spoofing
(D) SQL Injection

30. Which attack is based on sending malicious SQL queries?
(A) Brute force attack
(B) Buffer overflow
(C) social engineering
(D) SQL Injection

31. Which of the following is NOT a defense mechanism?
(A) Antivirus software
(B) Firewalls
(C) Virus
(D) Intrusion Detection Systems

32. Script kiddies are:
(A) Professional hackers
(B) inexperienced attackers using pre-written tools
(C) Cybersecurity researchers
(D) Law enforcement officers

33. A ransomware attack typically:
(A) Encrypts files and demands payment
(B) Removes file
(C) Creates backup copies
(D) Protects system from malware

34. Spyware is designed to:
(A) Monitor user activities secretly
(B) Delete files from system
(C) Slow down networks
(D) Attack servers only

35. Adware mainly:
(A) Encrypts data
(B) Shows useful advertisements
(C) Steals login credentials
(D) Shows unwanted advertisements

36. Which of these attacks uses fake emails to confuse users?
(A) SQL Injection
(B) Phishing
(C) Brute Force
(D) DDoS

37. A brute-force attack is used to:
(A) Guess passwords with all possible combinations
(B) Encrypt data
(C) Bypass firewalls
(D) Launch DDoS attacks

38. Keyloggers are used to:
(A) Encrypt files
(B) Monitor keystrokes secretly
(C) Monitor network traffic
(D) Block websites

39. Man-in-the-middle (MITM) attacks involve:
(A) Directly destroying files
(B) Intercepting and altering communication between two parties
(C) Injecting malware into hardware
(D) Only brute-force cracking

40. The difference between worms and viruses is:
(A) Worms need host files, viruses do not
(B) Viruses need host files, worms spread independently
(C) Both require user action
(D) Neither requires software execution

41. Which attack exploits human psychology instead of technical vulnerabilities?
(A) Social engineering
(B) phishing
(C) DNS Spoofing
(D) DoS

42. Which is NOT a component of a wireless network?
(A) Access Point (AP)
(B) Client Devices
(C) Router
(D) USB Cable

43. Which of the following is a major advantage of wireless networks?
(A) High cost
(B) Flexibility and mobility
(C) Low security
(D) Wired infrastructure required

44. WEP stands for:
(A) Wireless Encryption Protocol
(B) Wired Equivalent Privacy
(C) Wireless Encrypted Privacy
(D) Wireless Equivalent Privacy

45. WPA stands for:
(A) Wireless Protected Access
(B) Wireless Protected Authorization
(C) Wireless Privacy Algorithm
(D) Wide Protected Access

46. WPA2 improves security using:
(A) password
(B) AES encryption
(C) WEP keys
(D) MD5 hashing

47. WPA3 offers:
(A) Weak password protection
(B) Improved encryption and protection against brute-force attacks
(C) No security updates
(D) Only legacy WEP support

48. Which attack jams wireless signals intentionally?
(A) Phishing
(B) Jamming Attack
(C) SQL Injection
(D) Man-in-the-middle

49. SIM card cloning mainly threatens:
(A) Laptops
(B) Mobile phone identity and network security
(C) Wi-Fi routers
(D) Firewalls

50. A rogue AP can allow attackers to:
(A) Capture credentials
(B) Inject malware
(C) Perform MITM attacks
(D) All of the above

51. Smartphone Pentest Framework (SPF) is used to:
(A) Encrypt wireless networks
(B) Perform penetration testing on mobile devices
(C) Track lost phones
(D) Block malware automatically

52. The main threat to Android devices is:
(A) Trojan horse apps and malware
(B) WEP encryption
(C) MAC spoofing
(D) SSID broadcasting

53. Malware means:
(A) Malpracticed software
(B) multiset software
(C) malicious software
(D) all the above

54. Mobile security threats include:
(A) Malware apps
(B) Unprotected Wi-Fi connections
(C) Data leakage
(D) All of the above

55. Which of the following is a best practice for wireless security?
(A) Use strong WPA2/WPA3 passwords
(B) Disable default credentials
(C) Enable network monitoring
(D) All of the above

56. ISO 27001 is primarily concerned with:
(A) Software development standards
(B) Information security management systems (ISMS)
(C) Network hardware protocols
(D) Ethical hacking

57. Which of the following is NOT part of ISO 27001 clauses?
(A) Security policy
(B) Organization of information security
(C) Physical and environmental security
(D) Software programming practice standard

58. The IT Act, 2000 primarily regulates:
(A) Internet censorship
(B) Legal recognition of electronic records and digital signatures
(C) Hardware sales
(D) Telecommunication act

59. Section 66 of the IT Act 2000 addresses:
(A) Hacking and computer-related offenses
(B) Legal recognition of electronic records
(C) Copyright infringement
(D) Data protection only

60. Which international standard is widely used for cybersecurity risk management?
(A) ISO 14001
(B) ISO 9001
(C) ISO 27001
(D) ISO 50001

61. NIST cybersecurity framework is developed by:
(A) National Institute of Standards and Technology, USA
(B) National Institute of Standards and Technology,EU
(C) CERT-In, India
(D) ISO

62. NIST framework consists of:
(A) Identify, Protect, Detect, Respond, Recover
(B) Encrypt, Decrypt, Authenticate, Authorize
(C) Audit, Control, Monitor, Report
(D) None of the above

63. Security audit involves:
(A) Evaluating the effectiveness of security policies and controls
(B) Developing new software
(C) Monitoring only firewalls
(D) Ethical hacking only

64. Chain of custody in cyber forensics ensures:
(A) Secure network encryption
(B) custody of hacker to court
(C) Password protection
(D) Evidence integrity from collection to court

65. CERT-In in India is responsible for:
(A) Cybersecurity incident response
(B) Ethical hacking certification
(C) Hardware testing
(D) Software sales

66. Which of the following is considered a cybercrime under IT Act?
(A) Identity theft
(B) Phishing
(C) Hacking
(D) All of the above

67. Digital evidence in cyber investigations must be:
(A) Altered for analysis
(B) Collected in a forensically sound manner
(C) Stored only on USB drives
(D) Kept secret from courts

68. International cooperation in cybercrime is essential because:
(A) Ethical hacking is illegal
(B) Laws are identical worldwide
(C) Only local police can investigate
(D) Cybercrimes may cross borders

69. Investigation agencies use cyber forensics to:
(A) Recover deleted data
(B) Track hacker activity
(C) Preserve evidence for court
(D) All of the above

70. Security standards like ISO 27001 help organizations:
(A) Increase revenue directly
(B) enhance information security management and risk assessment
(C) Eliminate malware completely
(D) Replace antivirus software

71. Security management in IT primarily focuses on:
(A) Protecting only physical assets
(B) Protecting password
(C) Only updating software
(D) Protecting information, devices, and networks

72. Disaster recovery planning (DRP) is meant to:
(A) Increase internet speed
(B) Ensure business continuity after a disaster
(C) Block viruses
(D) Improve software coding

73. Business continuity planning differs from disaster recovery planning as:
(A) It deals with maintaining operations during disruption, not just IT recovery
(B) It focuses only on backup systems
(C) It prevents malware
(D) It only applies to financial institutions

74. Which of the following is NOT a phase of disaster recovery planning?
(A) Risk assessment
(B) Business impact analysis
(C) Malware installation
(D) Recovery strategy development

75. Digital signatures are based on:
(A) Symmetric encryption
(B) public key cryptogtaphy
(C) Hashing only
(D) Firewall rules

76. In digital signatures, the role of the hash function is to:

(A) Encrypt the entire message

(B) Compress the message into a fixed-size digest

(C) Generate the public/private key pair

(D) Store the message securely

77. Ethical hacking refers to:

(A) Unauthorized hacking for personal gain

(B) Authorized testing of systems to find vulnerabilities

(C) Writing malware

(D) Blocking network traffic

78. White-hat hackers are:

(A) Malicious hackers

(B) Ethical hackers

(C) Script kiddies

(D) Unauthorized intruders

79. Black-hat hackers are:

(A) Malicious hackers with destuctive intention

(B) Malicious hackers with good intention

(C) System administrators

(D) Cybersecurity auditors

80. Grey-hat hackers:

(A) Operate without permission but usually without malicious intent

(B) Always illegal

(C) Only write software

(D) Only test hardware

81. Penetration testing is:

(A) Monitoring network only

(B) Simulating attacks to know the system vulnerabilities

(C) Writing encryption algorithms

(D) Installing antivirus

82. Black-box penetration testing means:

(A) Tester knows all system details

(B) Tester has no prior knowledge of the system

(C) Tester modifies source code

(D) Tester only monitors logs

83. White-box penetration testing involves:

(A) No knowledge of the system

(B) knowledge of firewall configuration

(C) Only external attacks

(D) complete knowledge of system architecture

84. Computer forensics is about:
(A) Analysis of software code
(B) Investigation and preservation of digital evidence
(C) Writing malware
(D) Only network monitoring

85. Risk management in security management involves:
(A) password verification
(B) Installing antivirus only
(C) Updating software
(D) Identifying, assessing, and mitigating risks

86. Incident response refers to:
(A) Reacting to natural disasters only
(B) Responding to security incidents effectively
(C) Installing firewalls
(D) Encrypting emails

87. Digital signature verification ensures:
(A) Data integrity and non-repudiation
(B) Faster network connection
(C) Firewall protection
(D) Malware scanning

88. Ethical hacking is legal in a situation , when:
(A) Performed without consent
(B) Performed with authorization
(C) Always performed on competitors' systems
(D) Only for personal knowledge

89. Disaster recovery (DR) testing is required to:
(A) Evaluate effectiveness of the DR plan
(B) Install antivirus
(C) Update operating systems
(D) Encrypt network traffic

90. Which of the following is NOT a principle of the CIA triad in information security?
(A) Confidentiality
(B) Integrity
(C) Authentication
(D) Availability

91. DOS attack is an attack on which of the following service:
(A) Confidentiality
(B) Integrity
(C) Authentication
(D) Availability

92. The process of converting plain text into cipher text is called:
(A) Hashing
(B) Encryption
(C) Decryption
(D) Encoding

93. To get a digital signature, which key is used to encrypt a message?
(A) Public Key of the sender
(B) Private Key of the sender
(C) Public Key of the receiver
(D) Private Key of the receiver

94. For confidentiality of a message, , which key is used to encrypt a message?
(A) Public Key of the sender
(B) Private Key of the sender
(C) Public Key of the receiver
(D) Private Key of the receiver

95. What does multi-factor authentication (MF(A) improve?
(A) System speed
(B) User convenience
(C) Security by requiring multiple proofs of identity
(D) Encryption strength

96. Which of the following attacks attempts to inject malicious code into a website input field?
(A) Cross-Site Scripting (XSS)
(B) Brute Force
(C) DDoS
(D) Social Engineering

97. Why are passwords often stored as hashes rather than plaintext?
(A) To reduce storage requirements
(B) To make brute-force attacks easier
(C) To prevent exposure of actual passwords if the database is compromised
(D) To allow reversible encryption for recovery

98. What attack exploits weaknesses in hash functions by finding two different inputs with the same hash?
(A) Replay attack
(B) Collision attack
(C) Phishing attack
(D) Side-channel attack

99. Which of these is an example of a cryptographic hash algorithm?
(A) RSA
(B) AES
(C) SHA-256
(D) Diffie-Hellman

100. Which of the following best describes a one-way hash function in security?
(A) A function that allows both encryption and decryption using the same key
(B) the fixed-size output after applying hash function cannot be reversed to obtain the original input
(C) A function that uses symmetric keys to secure communication
(D) A function that generates random numbers for cryptographic use

Rough Work

Rough Work

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।