Roll. No. .....

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

Question Booklet Number

B.Sc. (FYUP)/B.Sc. (Hons.) (Biotech.) (SEM.-II) EXAMINATION, 2025-26

VOCATIONAL COURSE

CYBER SECURITY

[CODE : VOC-160]

Paper Code							
A	9	0	1	0	2	6	T

Question Booklet Series

C

Time : 1 : 00 Hour **Max. Marks : 60**

Instructions to the Examinee :

1. Do not open the booklet unless you are asked to do so.
2. The booklet contains 60 questions. Examinee is required to answer all 60 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 60 प्रश्न हैं। परीक्षार्थी को सभी 60 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. What is SSL/TLS?

(A) Programming language

(B) Hardware device

(C) Encryption protocol

(D) Antivirus

2. Digital device security refers to:

(A) Protecting physical devices only

(B) Protecting devices from cyber threats

(C) Data entry

(D) Printing Documents

3. Antivirus software is used to:

(A) Detect and remove malware

(B) Create viruses

(C) Increase RAM

(D) Manage files

4. What is device authentication?

(A) Deleting files

(B) Verifying identity of user/ device

(C) Installing software

(D) Connecting internet

5. Which is an example of biometric authentication?

(A) PIN

(B) Password

(C) Fingerprint

(D) Username

1. SSL/TLS क्या है?

(A) प्रोग्रामिंग भाषा

(B) हार्डवेयर डिवाइस

(C) एन्क्रिप्शन प्रोटोकॉल

(D) एंटीवायरस

2. डिज़िटल डिवाइस सुरक्षा का अर्थ है :

(A) केवल भौतिक उपकरणों की सुरक्षा करना

(B) उपकरणों को साइबर खतरों से बचाना

(C) डेटा प्रविष्टि

(D) दस्तावेज़ों को प्रिंट करना

3. एंटीवायरस सॉफ्टवेयर का उपयोग किया जाता है:

(A) मैलवेयर का पता लगाने और उसे हटाने के लिए

(B) वायरस बनाने के लिए

(C) RAM बढ़ाने के लिए

(D) फ़ाइलों को व्यवस्थित करने के लिए

4. डिवाइस ऑथेंटिकेशन क्या है?

(A) फ़ाइलें हटाना

(B) उपयोगकर्ता/डिवाइस की पहचान सत्यापित करना

(C) सॉफ़्टवेयर इंस्टॉल करना

(D) इंटरनेट से जुड़ना

5. बायोमेट्रिक प्रमाणीकरण का एक उदाहरण कौन-सा है?

(A) PIN

(B) पासवर्ड

(C) फिंगरप्रिंट

(D) यूज़रनेम

6. Intellectual property theft refers to:

(A) Copying legal documents

(B) Stealing creative work

(C) Backup files

(D) Data deletion

7. Which is a preventive measure against cybercrime?

(A) Regular software updates

(B) Weak passwords

(C) Sharing credentials

(D) Ignoring alerts

8. Data protection refers to:

(A) Data deletion

(B) Safeguarding data from unauthorized access

(C) Data copying

(D) Data formatting

9. Encryption is the process of:

(A) Deleting data

(B) Compressing data

(C) Copying data

(D) Converting data into unreadable form

10. Decryption is:

(A) Encoding data

(B) Decoding encrypted data

(C) Deleting data

(D) Storing data

6. बौद्धिक संपदा की चोरी का तात्पर्य है :

(A) कानूनी दस्तावेजों की नकल करना

(B) रचनात्मक कार्य की चोरी करना

(C) बैकअप फ़ाइलें

(D) डेटा हटाना

7. साइबर अपराध के विरुद्ध निवारक उपाय कौन-सा है?

(A) नियमित सॉफ्टवेयर अपडेट

(B) कमज़ोर पासवर्ड

(C) क्रेडेंशियल्स साझा करना

(D) अलर्ट्स को नज़रअंदाज़ करना

8. डेटा सुरक्षा का तात्पर्य है :

(A) डेटा हटाना

(B) अनधिकृत पहुँच से डेटा को सुरक्षित रखना

(C) डेटा की प्रतिलिपि बनाना

(D) डेटा फ़ॉर्मेटिंग

9. एन्क्रिप्शन एक प्रक्रिया है :

(A) डेटा को मिटाने की

(B) डेटा को कंप्रेस करने की

(C) डेटा को कॉपी करने की

(D) डेटा को न पढ़े जा सकने वाले रूप में बदलने की

10. Decryption है :

(A) डेटा को एनकोड करना

(B) एनक्रिप्टेड डेटा को डिकोड करना

(C) डेटा को डिलीट करना

(D) डेटा को स्टोर करना

11. Application security refers to:

(A) Protecting hardware

(B) Securing software applications from threats

(C) Managing networks

(D) Data entry

12. SQL Injection attacks target:

(A) Operating system

(B) Hardware

(C) Network cables

(D) Database queries

13. Authorization determines:

(A) Who can access resources

(B) Data encryption

(C) System speed

(D) Network connection

14. What is session management?

(A) Data storage

(B) Managing user sessions securely

(C) Data backup

(D) File compression

15. Which protects data in transit?

(A) Encryption

(B) Backup

(C) Deletion

(D) Formatting

11. एप्लीकेशन सुरक्षा का तात्पर्य है :

(A) हार्डवेयर की सुरक्षा करना

(B) सॉफ्टवेयर एप्लीकेशनों को खतरों से सुरक्षित करना

(C) नेटवर्क का प्रबंधन करना

(D) डेटा प्रविष्टि

12. SQL इंजेक्शन हमले किसे निशाना बनाते हैं ?

(A) ऑपरेटिंग सिस्टम

(B) हार्डवेयर

(C) नेटवर्क केबल

(D) डेटाबेस क्वेरी

13. Authorization यह निर्धारित करता है :

(A) संसाधनों तक कौन पहुँच सकता है

(B) डेटा एन्क्रिप्शन

(C) सिस्टम की गति

(D) नेटवर्क कनेक्शन

14. सेशन मैनेजमेंट क्या है ?

(A) डेटा स्टोरेज

(B) यूज़र सेशन को सुरक्षित रूप से मैनेज करना

(C) डेटा बैकअप

(D) फ़ाइल कम्प्रेशन

15. डेटा को ट्रांज़िट के दौरान कौन सुरक्षित रखता है ?

(A) एन्क्रिप्शन

(B) बैकअप

(C) डिलीशन

(D) फ़ॉर्मेटिंग

16. Cybercrime refers to:

(A) Physical crime

(B) Software testing

(C) Banking process

(D) Crime using computers or internet

17. Identity theft involves:

(A) Stealing hardware

(B) Stealing personal information

(C) Deleting files

(D) Encrypting data

18. Cyber stalking involves:

(A) Monitoring systems

(B) Network design

(C) Data encryption

(D) Online harassment

19. Online fraud includes:

(A) Safe transactions

(B) Deceptive financial activities

(C) Antivirus updates

(D) Data backup

20. Cyber bullying is:

(A) Online harassment or abuse

(B) Encouragement

(C) Data sharing

(D) Programming

16. साइबर अपराध का तात्पर्य है :

(A) शारीरिक अपराध

(B) सॉफ्टवेयर टेस्टिंग

(C) बैंकिंग प्रक्रिया

(D) कंप्यूटर या इंटरनेट का उपयोग करके किया गया अपराध

17. पहचान की चोरी में शामिल है :

(A) हार्डवेयर चुराना

(B) निजी जानकारी चुराना

(C) फ़ाइलें मिटाना

(D) डेटा को एन्क्रिप्ट करना

18. साइबर स्टॉकिंग में शामिल है :

(A) मॉनिटरिंग सिस्टम

(B) नेटवर्क डिज़ाइन

(C) डेटा एन्क्रिप्शन

(D) ऑनलाइन उत्पीड़न

19. ऑनलाइन धोखाधड़ी में शामिल हैं :

(A) सुरक्षित लेन-देन

(B) धोखेबाज़ वित्तीय गतिविधियाँ

(C) एंटीवायरस अपडेट

(D) डेटा बैकअप

20. साइबर बुलिंग है :

(A) ऑनलाइन उत्पीड़न या दुर्व्यवहार

(B) प्रोत्साहन

(C) डेटा साझा करना

(D) प्रोग्रामिंग

21. Network security means:

(A) Protecting hardware

(B) Protecting network from unauthorized access

(C) Creating websites

(D) Data entry

22. Which protocol is secure?

(A) HTTP

(B) FTP

(C) HTTPS

(D) Telnet

23. What is Network Sniffing?

(A) Data encryption

(B) Monitoring network traffic

(C) Data deletion

(D) File compression

24. What is MAC address?

(A) Software address

(B) Network attack

(C) IP protocol

(D) Unique hardware address

25. What is IP address?

(A) Device password

(B) Unique identifier of device on network

(C) Hardware device

(D) Security key

21. नेटवर्क सुरक्षा का अर्थ है :

(A) हार्डवेयर की सुरक्षा करना

(B) नेटवर्क को अनधिकृत पहुँच से सुरक्षित रखना

(C) वेबसाइट बनाना

(D) डेटा एंट्री

22. कौन-सा प्रोटोकॉल सुरक्षित है?

(A) HTTP

(B) FTP

(C) HTTPS

(D) Telnet

23. नेटवर्क स्निफ़िंग क्या है?

(A) डेटा एन्क्रिप्शन

(B) नेटवर्क ट्रैफ़िक की निगरानी

(C) डेटा हटाना

(D) फ़ाइल कम्प्रेशन

24. MAC एड्रेस क्या है?

(A) सॉफ्टवेयर एड्रेस

(B) नेटवर्क अटैक

(C) IP प्रोटोकॉल

(D) यूनिक हार्डवेयर एड्रेस

25. IP एड्रेस क्या है ?

(A) डिवाइस का पासवर्ड

(B) नेटवर्क पर डिवाइस की एक यूनिक पहचान

(C) हार्डवेयर डिवाइस

(D) सिक्योरिटी की

26. Phishing is:

(A) Data backup

(B) Fraudulent attempt to obtain sensitive data

(C) Encryption method

(D) Software testing

27. Spear Phishing targets:

(A) Random users

(B) Specific individuals or organizations

(C) Only banks

(D) Only students

28. Which is a sign of phishing?

(A) Official domain

(B) Secure connection

(C) Suspicious links

(D) Known sender

29. Pharming redirects users to:

(A) Secure websites

(B) Fake websites

(C) Antivirus tools

(D) Firewalls

30. Vishing involves:

(A) Email fraud

(B) SMS fraud

(C) Voice calls

(D) Websites

26. फ़िशिंग है :

(A) डेटा बैकअप

(B) संवेदनशील डेटा प्राप्त करने का एक धोखाधड़ी भरा प्रयास

(C) एन्क्रिप्शन विधि

(D) सॉफ़्टवेयर परीक्षण

27. स्पीयर फ़िशिंग लक्ष्यित करता है :

(A) रैंडम यूज़र्स

(B) विशिष्ट व्यक्ति या संगठन

(C) केवल बैंक

(D) केवल छात्र

28. फ़िशिंग का संकेत कौन-सा है?

(A) आधिकारिक डोमेन

(B) सुरक्षित कनेक्शन

(C) संदिग्ध लिंक

(D) ज्ञात प्रेषक

29. Pharming यूज़र्स को इन पर रीडायरेक्ट करता है :

(A) सुरक्षित वेबसाइटें

(B) नकली वेबसाइटें

(C) एंटीवायरस टूल्स

(D) फ़ायरवॉल

30. Vishing में शामिल है :

(A) ईमेल धोखाधड़ी

(B) SMS धोखाधड़ी

(C) वॉइस कॉल

(D) वेबसाइटें

31. What is a process in OS?

(A) Hardware

(B) Running program

(C) File

(D) Network

32. What is Kernel mode?

(A) User mode

(B) Restricted access mode

(C) Privileged mode with full access

(D) Safe mode

33. Which protects memory from unauthorized access?

(A) Memory protection

(B) File system

(C) Backup

(D) Antivirus

34. What is Sandboxing?

(A) File storage

(B) Running programs in isolated environment

(C) Data encryption

(D) Network design

35. What is Secure Boot?

(A) Fast boot

(B) Boot process ensuring trusted software loads

(C) Restart process

(D) Shutdown process

31. OS में प्रोसेस क्या है ?

(A) हार्डवेयर

(B) रनिंग प्रोग्राम

(C) फ़ाइल

(D) नेटवर्क

32. कर्नेल मोड क्या है ?

(A) यूज़र मोड

(B) सीमित एक्सेस मोड

(C) पूर्ण एक्सेस वाला विशेषाधिकार प्राप्त मोड

(D) सेफ़ मोड

33. मेमोरी को अनधिकृत पहुँच से कौन सुरक्षित रखता है ?

(A) मेमोरी सुरक्षा

(B) फ़ाइल सिस्टम

(C) बैकअप

(D) एंटीवायरस

34. सैंडबॉक्सिंग क्या है ?

(A) फ़ाइल स्टोरेज

(B) प्रोग्राम्स को एक अलग वातावरण में चलाना

(C) डेटा एन्क्रिप्शन

(D) नेटवर्क डिज़ाइन

35. सिक्योर बूट क्या है ?

(A) फास्ट बूट

(B) बूट प्रक्रिया जो यह सुनिश्चित करती है कि केवल विश्वसनीय सॉफ्टवेयर ही लोड हो

(C) रीस्टार्ट प्रक्रिया

(D) शटडाउन प्रक्रिया

36. Malware refers to:

(A) Safe software

(B) Hardware too

(C) Network device

(D) Malicious software

37. A virus attaches itself to:

(A) Network cables

(B) Files and programs

(C) Routers

(D) Databases

38. Ransomware is used to:

(A) Speed up systems

(B) Lock data and demand payment

(C) Delete antivirus

(D) Monitor users

39. Spyware is designed to:

(A) Show ads

(B) Encrypt data

(C) Destroy files

(D) Monitor user activities

40. A keylogger records:

(A) Screen resolution

(B) Network speed

(C) Keystrokes

(D) Password encryption

36. मालवेयर का अर्थ है :

(A) सुरक्षित सॉफ्टवेयर

(B) हार्डवेयर भी

(C) नेटवर्क डिवाइस

(D) दुर्भावनापूर्ण सॉफ्टवेयर

37. एक वायरस किससे जुड़ जाता है ?

(A) नेटवर्क केबल

(B) फ़ाइलें और प्रोग्राम

(C) राउटर

(D) डेटाबेस

38. रैनसमवेयर का उपयोग किसलिए किया जाता है ?

(A) सिस्टम की गति बढ़ाने के लिए

(B) डेटा को लॉक करने और भुगतान की माँग करने के लिए

(C) एंटीवायरस को हटाने के लिए

(D) उपयोगकर्ताओं की निगरानी करने के लिए

39. स्पाइवेयर को इस प्रकार डिज़ाइन किया जाता है कि वह :

(A) विज्ञापन दिखाए

(B) डेटा को एन्क्रिप्ट करे

(C) फ़ाइलों को नष्ट करे

(D) उपयोगकर्ता की गतिविधियों पर नज़र रखे

40. एक कीलॉगर रिकॉर्ड करता है :

(A) स्क्रीन रिज़ॉल्यूशन

(B) नेटवर्क की गति

(C) कीस्ट्रोक्स

(D) पासवर्ड एन्क्रिप्शन

41. What is Brute Force attack?

(A) Guessing passwords repeatedly

(B) Encrypting data

(C) Data backup

(D) Network design

42. What is a Vulnerability?

(A) Security weakness

(B) Strong password

(C) Antivirus

(D) Backup

43. Which mechanism restricts user access in OS?

(A) Access control

(B) File deletion

(C) Formatting

(D) Backup

44. What is a user account in OS?

(A) Hardware device

(B) Identity for system access

(C) File type

(D) Network cable

45. Which permission allows running a program?

(A) Read

(B) Write

(C) Execute

(D) Delete

41. ब्रूट फ़ोर्स अटैक क्या है ?

(A) बार-बार पासवर्ड का अंदाज़ा लगाना

(B) डेटा को एन्क्रिप्ट करना

(C) डेटा बैकअप

(D) नेटवर्क डिज़ाइन

42. कमजोरी क्या है ?

(A) सुरक्षा में कमी

(B) मज़बूत पासवर्ड

(C) एंटीवायरस

(D) बैकअप

43. OS में उपयोगकर्ता की पहुँच को कौन-सी प्रणाली प्रतिबंधित करती है ?

(A) पहुँच नियंत्रण

(B) फ़ाइल विलोपन

(C) फ़ॉर्मेटिंग

(D) बैकअप

44. OS में यूज़र अकाउंट क्या है ?

(A) हार्डवेयर डिवाइस

(B) सिस्टम एक्सेस के लिए पहचान

(C) फ़ाइल का प्रकार

(D) नेटवर्क केबल

45. कौन-सी अनुमति किसी प्रोग्राम को चलाने की अनुमति देती है ?

(A) Read

(B) Write

(C) Execute

(D) Delete

46. What is a Firewall?

(A) A physical wall

(B) Antivirus

(C) Database

(D) Network security system

47. What is Social Engineering?

(A) Software coding

(B) Manipulating people to get information

(C) Network design

(D) Data encryption

48. What is Authentication?

(A) Data deletion

(B) Virus removal

(C) Network attack

(D) Verifying identity

49. Which is used for authentication?

(A) Username and Password

(B) Firewall

(C) Router

(D) Switch

50. What is VPN?

(A) Virtual Private Network

(B) Virus Protection Network

(C) Virtual Public Node

(D) Verified Private Node

46. फ़ायरवॉल क्या है ?

(A) एक भौतिक दीवार

(B) एंटीवायरस

(C) डेटाबेस

(D) नेटवर्क सुरक्षा प्रणाली

47. सोशल इंजीनियरिंग क्या है ?

(A) सॉफ्टवेयर कोडिंग

(B) जानकारी हासिल करने के लिए लोगों को मैनिपुलेट करना

(C) नेटवर्क डिज़ाइन

(D) डेटा एन्क्रिप्शन

48. Authentication क्या है ?

(A) डेटा हटाना

(B) वायरस हटाना

(C) नेटवर्क हमला

(D) पहचान की पुष्टि करना

49. प्रमाणीकरण के लिए किसका उपयोग किया जाता है ?

(A) यूज़रनेम और पासवर्ड

(B) फ़ायरवॉल

(C) राउटर

(D) स्विच

50. VPN क्या है ?

(A) वर्चुअल प्राइवेट नेटवर्क

(B) वायरस प्रोटेक्शन नेटवर्क

(C) वर्चुअल पब्लिक नोड

(D) वैरिफाइड प्राइवेट नोड

51. Which is an example of symmetric encryption?

(A) AES

(B) RSA

(C) HTTPS

(D) SSL

52. What is a public key?

(A) Secret key

(B) Shared openly for encryption

(C) Stored offline only

(D) Used only for decryption

53. Which ensures data is not altered?

(A) Confidentiality

(B) Backup

(C) Availability

(D) Integrity

54. What is Hashing?

(A) Encryption with key

(B) Data backup

(C) One-way conversion of data

(D) File compression

55. Digital signature is used for:

(A) Data storage

(B) Authentication and integrity

(C) Data deletion

(D) File compression

51. सिमेट्रिक एन्क्रिप्शन का एक उदाहरण कौन-सा है?

(A) AES

(B) RSA

(C) HTTPS

(D) SSL

52. पब्लिक की क्या है?

(A) सीक्रेट की

(B) एन्क्रिप्शन के लिए खुले तौर पर शेयर की जाती है

(C) केवल ऑफ़लाइन स्टोर की जाती है

(D) केवल डिक्रिप्शन के लिए इस्तेमाल की जाती है

53. कौन यह सुनिश्चित करता है कि डेटा में कोई बदलाव न हो?

(A) गोपनीयता

(B) बैकअप

(C) उपलब्धता

(D) अखंडता

54. हैशिंग क्या है?

(A) कुंजी के साथ एन्क्रिप्शन

(B) डेटा बैकअप

(C) डेटा का एक-तरफ़ा रूपांतरण

(D) फ़ाइल संपीड़न

55. डिज़िटल हस्ताक्षर का उपयोग किसके लिए किया जाता है?

(A) डेटा भंडारण

(B) प्रमाणीकरण और अखंडता

(C) डेटा विलोपन

(D) फ़ाइल संपीड़न

56. What is Cyber Security?

(A) Protection of physical devices

(B) Protection of internet-connected systems

(C) Data entry process

(D) Software development

57. Which of the following is a common cyber threat?

(A) Firewall

(B) Antivirus

(C) Malware

(D) Backup

58. What does CIA triad stand for?

(A) Control, Integrity, Access

(B) Confidentiality, Integrity, Availability

(C) Cyber, Internet, Access

(D) Code, Information, Access

59. Which attack tries to flood a system with traffic?

(A) Phishing

(B) Spoofing

(C) DDoS

(D) Sniffing

60. Which protocol is secure?

(A) HTTP

(B) FTP

(C) HTTPS

(D) Telnet

56. साइबर सुरक्षा क्या है ?

(A) भौतिक उपकरणों की सुरक्षा

(B) इंटरनेट से जुड़े सिस्टम की सुरक्षा

(C) डेटा एंट्री प्रक्रिया

(D) सॉफ्टवेयर विकास

57. निम्नलिखित में से कौन-सा एक सामान्य साइबर खतरा है ?

(A) फ़ायरवॉल

(B) एंटीवायरस

(C) मालवेयर

(D) बैकअप

58. CIA triad का क्या अर्थ है ?

(A) Control, Integrity, Access

(B) Confidentiality, Integrity, Availability

(C) Cyber, Internet, Access

(D) Code, Information, Access

59. कौन-सा हमला किसी सिस्टम को ट्रैफिक से भर देने की कोशिश करता है ?

(A) फ़िशिंग

(B) स्पूफ़िंग

(C) DDoS

(D) स्निफ़िंग

60. कौन-सा प्रोटोकॉल सुरक्षित है ?

(A) HTTP

(B) FTP

(C) HTTPS

(D) Telnet

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।