

National Forensic Sciences University
Scientific Assistant - Cyber & TASI - Gr. C (Contractual Basis)
Directorate of Forensic Science Laboratory, Home Department, State
of Maharashtra

Examination type: MCQ
Revised Final Answer Key

Date: 4th May 2025

Instructions:

1. Multiple Choice Question Examination.
2. Chose the correct answer and mark in the OMR sheet with black ball pen.
3. No-negative marking and each question carry one marks.
4. Duration of the paper is 60 minutes

Q-1 Answer the following Question

[Marks: 60]

1. Which of the following is a *non-volatile* primary storage device?
A) RAM **B) ROM** C) Cache D) Register
2. Which of the following correctly describes an algorithm?
A) A specific programming language code **B) A detailed sequence of steps to solve a problem**
C) A machine-level instruction set D) A hardware abstraction layer
3. Which data structure is *best* suited for implementing a "First-In-First-Out" (FIFO) behavior?
A) Stack **B) Queue** C) Tree D) Graph
4. In an Operating System, the *process state* where a process is waiting for some event to occur (like I/O completion) is called:
A) Running B) Ready **C) Waiting** D) Terminated
5. Which of the following file systems supports journaling, making it more resilient to crashes?
A) FAT32 **B) NTFS** C) CDFS D) ExFAT
6. Which of the following is NOT a property of a relational database?
A) Data is stored in tables B) Relationships are established using foreign keys
C) Data is stored as unstructured documents D) SQL is used for querying
7. Which of the following best represents the principle of *Least Privilege* in cybersecurity?
A) Providing all users with administrative access
B) Allowing users access only to the resources necessary for their role

- C) Giving temporary access to all system files
D) Sharing passwords among team members for easier collaboration
8. In the context of access control, what does *Authentication* verify?
A) The permissions of a user
B) The identity of a user
C) The number of active sessions
D) The encryption strength of the password
9. Which of the following uses **two different keys** for encryption and decryption?
A) Advanced Encryption Standard (AES)
B) Data Encryption Standard (DES)
C) RSA
D) Triple DES (3DES)
10. A malware that replicates itself and spreads without the need for user action is classified as:
A) Trojan Horse
B) Ransomware
C) Worm
D) Rootkit
11. Which of the following hash algorithms is considered the most secure among the options listed?
A) MD5
B) SHA-1
C) SHA-2
D) None of these
12. In cross-border cybercrime investigations, a **Letter Rogatory** is used to:
A) Arrest a suspect without a warrant
B) Request information from a foreign court
C) Encrypt confidential emails
D) Bypass national laws on surveillance
13. Which of the following is considered the **first cardinal rule** of digital forensics?
A) Always work on original evidence
B) Maintain chain-of-custody
C) Do not change the data
D) Use the latest forensic tools
14. Which step immediately follows the **identification** of digital evidence in the forensic process?
A) Acquisition
B) Analysis
C) Presentation
D) Reporting
15. Locard's Principle of Exchange implies that:
A) Digital evidence cannot be tampered with
B) Every contact leaves a trace
C) Only physical evidence is admissible
D) Electronic evidence self-destructs over time
16. Which of the following is **NOT** a commonly recognized branch of digital forensics?
A) Network forensics
B) Mobile device forensics
C) Underwater forensics
D) Cloud forensics
17. At a digital crime scene, what should the forensic examiner do first?
A) Shut down all devices immediately
B) Photograph and document the scene

- C) Start imaging hard drives directly D) Move all computers to a secure lab
18. The **Chain-of-Custody** refers to:
- A) Encrypting the evidence during transmission
 - B) Recording the chronological history of evidence handling
 - C) Using multiple investigators simultaneously
 - D) Keeping evidence at the crime scene until analysis
19. Write-blockers are used during evidence acquisition to:
- A) Speed up data transfer
 - B) Prevent accidental overwriting of source data
 - C) Format the evidence device
 - D) Encrypt the evidence for security
20. Which of the following statements correctly distinguishes **data recovery** from **data carving**?
- A) Data recovery retrieves deleted data using file system metadata; carving reconstructs files without metadata
 - B) Data recovery and data carving are identical processes
 - C) Carving is faster than recovery because it ignores file signatures
 - D) Data carving requires a full file system backup
21. Which of the following tools is **primarily used for disk imaging** in forensic investigations?
- A) Autopsy
 - B) FTK Imager
 - C) Wireshark
 - D) EnCase Examiner
22. Which file system is commonly used in modern Mac OS devices for better encryption and performance?
- A) HFS+
 - B) FAT32
 - C) APFS
 - D) NTFS
23. In Windows systems, which registry hive stores information about system-wide software configurations?
- A) HKEY_CURRENT_USER
 - B) HKEY_LOCAL_MACHINE
 - C) HKEY_CLASSES_ROOT
 - D) HKEY_USERS
24. Slack space in a file system refers to:
- A) Unused space in memory
 - B) Space between end of file and end of disk cluster
 - C) A temporary buffer for RAM
 - D) The file system's journal
25. In Linux, the permission "rwxr-xr--" assigned to a file means:
- A) Owner has all permissions, group can execute only, others can write
 - B) Owner can read, write, and execute; group can read and execute; others can only read
 - C) Owner and group can only execute
 - D) Everyone can read and write
26. Which of the following folders in macOS contains system logs that can aid forensic investigations?
- A) /Applications
 - B) /System/Logs
 - C) /var/log
 - D) /Users/Logs

27. In web browser forensics, the file typically used to track recently visited websites is:
A) Bookmarks.db B) Cache.db C) History.db D) Sessions.db
28. In email header analysis, the "Received:" field is primarily used to:
A) Identify the sender's full name B) Track the path of an email through servers
C) Encrypt the message content D) Identify email attachments
29. When seizing a mobile phone, the first recommended step to prevent remote wiping is:
A) Turn off the device immediately B) Remove the SIM card
C) Enable airplane mode D) Start imaging the device
30. Which mobile acquisition method captures **all data**, including deleted files and unallocated space?
A) Logical acquisition B) Manual extraction
C) File system acquisition D) Physical acquisition
31. Which section of the IT Act 2000 specifically addresses the punishment for hacking?
A) Section 43 B) Section 66 C) Section 72 D) Section 79
32. Under the DPDP Act, 2023, what term is used for an individual whose personal data is being processed?
A) Data Processor B) Data Fiduciary C) Data Principal D) Data Auditor
33. Which international convention is widely considered the first treaty on crimes committed via the Internet?
A) Hague Convention B) Budapest Convention
C) Vienna Convention D) Geneva Convention
34. Which of the following best describes *Cyber Ethics*?
A) Study of hacking techniques B) Laws enforced in the cyber world
C) Moral principles guiding online behaviour D) Encryption rules for data protection
35. Which Act in India specifically deals with protection against child sexual offenses online and offline?
A) IT Act 2000 B) POCSO Act 2012 C) POSH Act 2013 D) Juvenile Justice Act 2015
36. Which of the following is a major *privacy concern* related to social media platforms?
A) Faster content delivery B) Exposure of personal information without consent
C) Increased server downtime D) Frequent software updates

37. खालीलपैकी शुद्ध शब्द कोणता आहे?

- a) फसवणुक
- b) फसवणूक
- c) फसावनूक
- d) फसावणुक

38. 'सर्वांना समज दिली जाईल' या वाक्याचा प्रयोग ओळखा.

- a) शक्यकर्मणी
- b) कर्मकर्तरी
- c) पुरुषकर्मणी
- d) भावकर्तरी

39. खालील विधाने वाचा व योग्य पर्याय निवडा.

- (1) जो विकारी शब्द नामाची व्याप्ती मर्यादित करतो त्यास विशेषण म्हणतात.
- (2) ज्या शब्दांपासून कालगत क्रियेचा बोध होतो त्या शब्दांस क्रियापदे असे म्हणतात.
- (3) सर्वनाम ही नामाप्रमाणे लिंग, वचन व विभक्ती विकार धारण करणारी शब्दजाती नाही तर ती स्वतंत्र आहे.

पर्यायी उत्तरे :

- a) (1) व (2) बरोबर
- b) (2) व (3) बरोबर
- c) (1) व (3) बरोबर
- d) (1), (2), (3) बरोबर

40. "पुरावा नाही" - या वाक्यात "पुरावा" ही संज्ञा कोणत्या प्रकारची आहे?

- a) क्रियावाचक
- b) गुणवाचक
- c) भाववाचक
- d) वस्तुवाचक

41. "पोलिसांनी चौकशी केली." - यामधील क्रियापद कोणते?

- a) चौकशी
- b) केली
- c) पोलिसांनी
- d) साक्ष

42. "गुन्हेगारी वाढली आहे." - यात 'वाढली आहे' हे कोणते प्रकारचे काळवाचक रूप आहे?

- a) भूत
- b) पूर्ण वर्तमान
- c) संयुक्त काळ
- d) आजार्थ

43. "तो खोटे बोलत होता." या वाक्याचे रचनेनुसार प्रकार कोणता आहे?
- संयुक्त वाक्य
 - मिश्र वाक्य
 - साधे वाक्य
 - प्रश्नवाचक वाक्य
44. "न्याय मिळाला पाहिजे." - या वाक्याचा प्रकार कोणता?
- आज्ञार्थ
 - विधान
 - इच्छार्थ
 - उद्देशार्थ
45. मराठीचा अभ्यास करताना कोणकोणत्या गोष्टींचा अभ्यास करणे आवश्यक असते ?
- (1) मराठीच्या प्रादेशिक बोलींचा
 - (2) जातिपरत्वे पडणाऱ्या भेदांचा
 - (3) प्रतिष्ठित वर्गाच्या भाषेचा
- पर्यायी उत्तरे :
- (1) व (3) बरोबर
 - (2) व (3) बरोबर
 - (1) व (2) बरोबर
 - (1), (2), (3) चूक
46. खालीलपैकी कोणता शब्द परिभाषिक आहे?
- गुन्हा
 - पुरावा
 - चौकशी
 - सायबर गुन्हा
47. "सत्यशोधन" या शब्दात कोणता समास आहे?
- तत्पुरुष
 - कर्मधारय
 - द्वंद्व
 - बहुव्रीहि
48. "न्यायालयाने शिक्षेचा निर्णय दिला." - वाक्यातील क्रियापद ओळखा:
- शिक्षेचा
 - निर्णय
 - दिला
 - न्यायालयाने

49. वाक्य पूर्ण करा:

"तो दोषारोप ____ तयार नव्हता."

a) स्विकारण्यास

b) दाखल करण्यास

c) ऐकण्यास

d) सांगण्यास

50. चुकीचे वाक्य ओळखा:

a) पोलिसांनी चौकशी पूर्ण केली.

b) आरोपीने शिक्षा पत्करली.

c) न्यायालयाने निर्णय दिला.

d) फॉरेन्सिकचा अहवाल येतील.

51. वाक्य शुद्ध करा:

"माझे नाव तपास यादीत आहे."

a) माझं नाव तपास यादीत आहे.

b) माझे नाव तपास यादीत आहे.

c) माझं नाव तपास यादीत होती.

d) माझं नाव तपास यादीत नव्हतं.

52. "तो निर्दोष असल्याचं सिद्ध झालं आहे." - या वाक्यातील काळ कोणता आहे?

a) भूत

b) पूर्ण वर्तमान

c) भविष्य

d) आजार्थ

53. मराठी भाषे संदर्भातील पुढील कोणते वाक्य अयोग्य आहे ?

a) 'मराठी असे आमुची मायबोली' असे प्रत्येक मराठी भाषिकाने अभिमानाने म्हटले पाहिजे.

b) मराठी महाराष्ट्र राज्याची राजभाषा आहे.

c) हिंदी ही मराठी भाषेची जननी आहे.

d) आज मराठी भाषेच्या लेखनासाठी देवनागरी लिपीचा वापर होतो.

54. "फॉरेन्सिक तपास महत्वाचा आहे." या वाक्यातील विशेषण कोणते आहे?

a) फॉरेन्सिक

b) तपास

c) आहे

d) महत्वाचा

55. वाक्य शुद्ध करा:

"तो गुन्हा मान्य केलाय."

- a) तो गुन्हा मान्य केलाय.
- b) त्याने गुन्हा मान्य केला आहे.
- c) गुन्हा तो मान्य केलाय.
- d) त्याने गुन्हा केलेला आहे

56. "तपास अधिकारी चौकशीत गुंतले आहेत." - यात क्रियापद कोणते आहे?

- a) तपास
- b) अधिकारी
- c) गुंतले
- d) चौकशीत

57. वाक्य पूर्ण करा:

"सायबर गुन्ह्यांमध्ये वाढ ____."

- a) होत आहे
- b) करतो आहे
- c) केली आहे
- d) संपली आहे

58. चुकीचे वाक्य ओळखा:

- a) तो एक जबाबदार अधिकारी आहे.
- b) कोर्टाने निर्णय दिला आहे.
- c) साक्षीदाराने सत्य बोलले नाही.
- d) पुरावे साक्षीदार दाखवत.

59. "न्याय मिळणे" - या संज्ञेचा अर्थ काय?

- a) शिक्षा देणे
- b) आरोप करणे
- c) योग्य निर्णय मिळणे
- d) चौकशी करणे

60. वाक्य शुद्ध करा:

"तो पोलिस चौकशीसाठी बोलवलेला आहे."

- a) तो पोलिस चौकशीसाठी बोलवलेला आहे.
- b) तो पोलिस चौकशीसाठी बोलावला आहे.
- c) तो पोलीस चौकशीसाठी बोलवलेला आहे.
- d) तो चौकशीसाठी पोलिस बोलावले.