(8 pages)

Reg. No. : .....

Code No. : 6035 **Sub. Code : WCAE 31**

M.C.A. (CBCS) DEGREE EXAMINATION, APRIL 2025.

Third Semester

Computer Applications

Elective V – CYBER SECURITY

(For those who joined in July 2023 onwards)

Time : Three hours Maximum : 75 marks

PART A — (15 × 1 = 15 marks)

Answer ALL questions.

Choose the correct answer :

1. Which of the following is not a type of malware?
   (a) Virus (b) Worm
   (c) Firewall (d) Trojan Horse

2. Which type of cybercrime involves stealing personal information to Commit fraud?
   (a) Phishing (b) Spoofing
   (c) Hacking (d) Identity Theft

3. Which of the following is used to verify the identity of a user in digital communication?
   (a) Firewall (b) Antivirus
   (c) Digital Signature (d) Steganography

4. What is a key security measure to protect a WLAN?
   (a) Using a shared password for all devices
   (b) Disabling encryption
   (c) Enabling WPA3 encryption
   (d) Allowing open access to the network

5. Which is a basic smartphone security guideline?
   (a) Disabling-the lock screen
   (b) Installing apps from unknown sources
   (c) Using simple passwords like "1234"
   (d) Regularly updating the operating system and apps

6. What benefit does two-step verification provide?
   (a) Simplifies the login, process
   (b) Adds an extra layer of security
   (c) Reduces the need for strong passwords
   (d) Makes passwords unnecessary

7. What does computer analysis for the hacker defender program involve?
   (a) Developing new hacking tools
   (b) Defending against hacking attempts
   (c) Educating hackers on cybersecurity
   (d) Analyzing and detecting rootkits used by hackers

8. What is a risk of eavesdropping on WiFi?
   (a) It is always secure
   (b) Unauthorized interception of private communications
   (c) Improving WiFi speed
   (d) Legal protection of intercepted data

9. What is the primary role of a cybercrime investigator?
   (a) To prosecute cyber criminals
   (b) To assist in incident response and analyze digital evidence
   (c) To legislate new cyber laws
   (d) To provide cybersecurity training to the public

10. What is a common thread within digital evidence seizure?
   (a) Ignoring the chain of custody
   (b) Preserving the integrity and authenticity of the evidence
   (c) Allowing unauthorized access to the evidence
   (d) Using non-standardized procedures

11. How can IP addresses be used in cybercrime investigations?
   (a) To replace digital evidence
   (b) To encrypt digital evidence
   (c) To destroy digital evidence
   (d) To physically locate a device involved in the crime

12. What is an essential skill for conducting cyber investigations?
   (a) Proficiency in physical combat
   (b) Knowledge of digital forensics and cybersecurity principles
   (c) Ability to code in all programming languages
   (d) Familiarity with all existing hardware

13. What is the primary focus of digital forensics?

(a) Developing new software applications

(b) Investigating and analyzing digital evidence for legal purposes

(c) Providing technical support to users

(d) Designing hardware components

14. During which phase of digital forensics is the data analyzed to draw conclusions?

(a) Collection

(b) Examination

(c) Reporting

(d) Analysis

15. Which of the following is a critical step during the collection phase of digital forensics?

(a) Modifying the data on the suspect device

(b) Preserving the integrity of the digital evidence

(c) Ignoring the chain of custody

(d) Analyzing the collected data immediately

PART B — (5 × 4 = 20 marks)

Answer ALL questions, choosing either (a) or (b).
Each answer should not exceed 250 words.

16. (a) Explain the different types of malware and explain each type.

Or

(b) Define the benefits of enabling two-step verification for online accounts.

17. (a) Mention some safe browsing guidelines for using social networking sites.

Or

(b) Explain the different measures can you take to ensure secure communication on your smartphone.

18. (a) Describe WiFi RF scanning, and why is it important in cyber investigations

Or

(b) How does the Fourth Amendment apply to the expectation of privacy in WLAN?

19. (a) Discuss how do investigators determine the most appropriate method for seizing digital evidence.

Or

(b) List some common misconceptions about computer/cybercrime.

20. (a) Briefly describe the evolution of computer forensics and how has the field changed over time?

Or

(b) Why cybercrime prevention is important and explains its strategies for preventing cybercrime?

PART C — (5 × 8 = 40 marks)

Answer ALL questions, choosing either (a) or (b)
Each answer should not exceed 600 words.

21. (a) Explain in brief about report cybercrimes with its challenges.

Or

(b) Provide an overview and effect of the key cybersecurity initiatives undertaken by the Indian government to combat cybercrime.

22. (a) Explain the essential email security tips that can protect users from phishing and other email-based attacks.

Or

(b) Explain what precautions should be taken during the setup and installation of apps on a smartphone.

23. (a) Examine the collaborative roles of law enforcement officers and cybercrime investigators in a cybererime investigation.

Or

(b) Describe the importance of network analysis in cybercrime investigations and how it identifying and tracing cybercriminal activities.

24. (a) Discuss common misconceptions about computer and cybercrime and how it affect public perception.

Or

(b) Analyze the impact of the explosion of networking on cybercrime and cyber investigations.

25. (a) Elaborate the four main phases of digital forensics with its best practices.

Or

(b) Illustrate the importance of cybercrime prevention and strategies.

———————