

Dr. Babasaheb Ambedkar Open University, Ahmedabad

Term-End Examination : January-2026

Course Name : BSCIT

Subject Name : Cyber Security

Subject Code : BSCITRIN-304

Date : 19-02-2026

Time : 03:00PM TO 05:15PM

Max Marks : 70

Section A

Q.-1. Respond to any three of the following questions in brief. (30)

- (1) Classify cyber crimes into different categories and explain the reasons behind their commission. Provide examples for each category.
- (2) Compare and contrast different types of malware such as viruses, worms, Trojans, and spyware. Explain their modes of operation and potential impacts.
- (3) Describe the major cyber security initiatives taken by the Government of India. Evaluate their effectiveness in protecting national critical infrastructure.
- (4) Discuss safe browsing guidelines for social networking sites. How can users protect their privacy and data while using platforms like Facebook and Twitter?
- (5) Elaborate on the phases of penetration testing, from foot printing to covering tracks. What tools and techniques are used in each phase?

Section B

Q.-2. Write short notes on any four of the following topics. (20)

- (1) List and briefly explain any five types of cyber crimes.
- (2) What is steganography? Explain its applications in cyber security with examples.
- (3) Summarize any two recent cyber crime incidents discussed in the unit.
- (4) What factors should be considered while choosing a web browser for secure browsing?
- (5) Differentiate between White Hat, Black Hat, and Grey Hat hackers.
- (6) What are the different types of penetration testing? Explain each briefly.

Section C

Q.-3. Multiple Choice Questions (10)

(1) What was ARPANET primarily designed to do?

- | | |
|---|--|
| A) Connect universities for research | B) Survive a nuclear attack by maintaining communication |
| C) Provide commercial internet services | D) Enable email communication |

(2) What does a White Hat hacker do?

- | | |
|------------------------------------|--------------------------------|
| A) Hacks for personal gain | B) Hacks with malicious intent |
| C) Hacks ethically with permission | D) Hacks without any purpose |

(3) What is the primary purpose of a digital signature?

- | | |
|---------------------------------|--|
| A) To hide data within images | B) To verify the authenticity and integrity of a message |
| C) To encrypt email attachments | D) To prevent phishing attacks |

(4) Why should cyber crimes be reported?

- | | |
|--------------------------------|--|
| A) To increase company profits | B) To help law enforcement track and prosecute criminals |
| C) To gain media attention | D) To avoid fixing security flaws |

(5) Which virus attacked Iran's nuclear facility in 2010?

- | | |
|------------|-------------|
| A) Xnet | B) Stuxnet |
| C) Melissa | D) Code Red |

(6) Which Indian agency is responsible for responding to cyber security incidents?

- | | |
|-----------|------------|
| A) NCRB | B) CERT-In |
| C) NCIIPC | D) DSCI |

(7) What is the main function of a firewall?

- A) To speed up internet connection
- B) To block all outgoing traffic
- C) To monitor and control network traffic
- D) To encrypt emails

(8) What should you avoid when using public Wi-Fi?

- A) Online shopping
- B) Accessing sensitive websites like banking
- C) Checking news websites
- D) Using social media

(9) What is a major risk of posting personal details on social media?

- A) Improved privacy
- B) Identity theft and targeting
- C) Increased friend requests
- D) Better ad targeting

(10) What makes SMS communication insecure?

- A) It is too slow
- B) It is not encrypted and can be easily intercepted
- C) It is too expensive
- D) It only works on certain phones

Section D

Q.-4. Decide whether the statements given below are True or False.

(10)

- (1) DNS translates domain names into IP addresses.
- (2) Worms can replicate themselves and spread across networks without user action.
- (3) Encryption is the process of converting readable data into an unreadable format using a key.
- (4) Computer forensics only deals with the recovery of data from computers, not smartphones.
- (5) India has more trained cyber security experts than the United States.
- (6) CERT-In was established in 2004 to respond to computer security incidents in India.
- (7) A strong password should be at least 8 characters long and include a mix of character types.
- (8) Password managers store all passwords in plain text for easy access.
- (9) Public Wi-Fi networks are generally safe for conducting online banking transactions.
- (10) SMS communication is considered a secure method for sending sensitive information.
