R2861	Sub. Code
	556201

M.Sc. DEGREE EXAMINATION, APRIL – 2025

Second Semester

Cyber Forensics

DISTRIBUTED OPERATING SYSTEM IN CYBER SPACE

(CBCS – 2023 onwards)

Time : 3 Hours   Maximum : 75 Marks
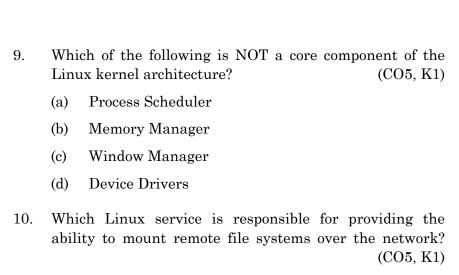
Part A   (10 × 1 = 10)

Answer **all** the objective questions by choosing the correct options.

1. Which of the following is a primary goal of a Distributed Operating System (DOS)? (CO1, K1)

   (a) Centralized control and management

   (b) Transparency of resources and communication

   (c) Maximizing the hardware failure

   (d) Simplification of user interfaces

2. In a Peer-to-Peer architecture of Distributed Operating System, the following statement is true: (CO1, K1)

   (a) One machine acts as a server while others are clients

   (b) All machines act as both clients and servers, without a centralized control

   (c) Only one machine is active in the system, others are idle

   (d) A master node governs the communication between all peers

3. Which of the following is an example of a message-oriented communication in a Distributed Operating System? (CO2, K1)

    (a) A process reading from a shared memory segment

    (b) A process calling a remote function using RPC

    (c) A process sending a message to another process through a communication channel

    (d) A process exchanging data with another process through a stream

4. In Distributed Operating Systems, which of the following communication types is typically used to invoke methods on remote objects in object oriented systems? (CO2, K1)

    (a) Message-oriented communication

    (b) Remote Procedure Call (RPC)

    (c) Remote Method Invocation (RMI)

    (d) Stream-oriented communication

5. Which of the following algorithms is used for synchronizing clocks in distributed systems by using a master clock that adjusts the local clocks of other machines? (CO3, K1)

    (a) Cristian's Algorithm

    (b) Lamport's Logical Clock

    (c) Network Time Protocol (NTP)

    (d) Berkeley Algorithm

R2861

6.	In Lamport's Logical Clock, the primary purpose of the clock is to: (CO3, K1)

(a)	Keep track of real-time across distributed nodes

(b)	Maintain the order of events in a distributed system

(c)	Synchronize the clocks of all nodes

(d)	Allow for precise timing of processes across different time zones

7.	Which of the following is a key advantage of Distributed Shared Memory (DSM) in Distributed Operating Systems? (CO4, K1)

(a)	It provides high availability by replicating data across all nodes

(b)	It ensures that all nodes have a globally synchronized clock

(c)	It allows processes to share memory locations across distributed systems as if they were on a single machine

(d)	It provides fault tolerance by distributing the computation load

8.	Which of the following is a challenge in implementing Distributed Shared Memory (DSM)? (CO4, K1)

(a)	Ensuring memory coherence across distributed nodes

(b)	Centralizing all memory management in one system

(c)	Limiting the use of caches across all processes

(d)	Using only synchronous communication for memory access

3

R2861

9. Which of the following is NOT a core component of the Linux kernel architecture? (CO5, K1)

    (a) Process Scheduler

    (b) Memory Manager

    (c) Window Manager

    (d) Device Drivers

10. Which Linux service is responsible for providing the ability to mount remote file systems over the network? (CO5, K1)

    (a) NFS (Network File System)

    (b) DNS (Domain Name System)

    (c) HTTPD (Apache Web Server)

    (d) SSH (Secure Shell)

Part B (5 × 5 = 25)

Answer **all** the questions not more than 500 words each.

11. (a) Describe the basic functions of a Distributed Operating System (DOS). (CO1, K2)

    Or

    (b) What are the major challenges faced in the design of Distributed Operating Systems. (CO1, K2)

12. (a) What are the key issues in communication within a Distributed Operating System? (CO2, K2)

    Or

    (b) Explain the concept of blocking vs non-blocking communication in a Distributed Operating System. (CO2, K2)

4

R2861

13. (a) Explain the importance of synchronization, clocks, and events in distributed systems. How do they affect the functioning of distributed applications? (CO3, K2)

Or

(b) Describe Cristian's Algorithm for clock synchronization in distributed systems. (CO3, K2)

14. (a) Explain the concept of memory coherence in Distributed Shared Memory (DSM) systems. Why is it important for consistency in distributed systems? (CO4, K2)

Or

(b) Discuss the challenges and advantages of using Distributed Shared Memory (DSM) in a Distributed Operating System. (CO4, K3)

15. (a) Describe the architecture of the Linux kernel. What are its primary components and how do they interact? (CO5, K2)

Or

(b) What services are offered by the Linux operating system? Briefly describe the functionality of each service. (CO5, K2)

5

R2861

Part C (5 × 8 = 40)

Answer **all** the questions not more than 1000 words each.

16. (a) Explain the different architectures of Distributed Operating Systems. Provide examples where each architecture is most suitable. (CO1, K3)

Or

(b) Analyse the concept of Inter-Process Communication (IPC) in Distributed Operating Systems. Explain its importance, types, and mechanisms used for IPC. (CO1, K4)

17. (a) Describe and compare the different types of communication mechanisms used in Distributed Operating Systems. (CO2, K3)

Or

(b) What is the difference between structured and unstructured communication in Distributed Operating Systems? Explain with examples. (CO2, K3)

18. (a) Discuss the Berkeley Algorithm and its role in synchronizing clocks in a distributed system. How does it differ from Cristian's Algorithm? (CO3, K2)

Or

(b) Explain the concepts of Logical Time and Logical Clocks. Discuss Lamport's Logical Clock and Vector Clock in detail. (CO3, K3)

R2861

19. (a) Explain the architecture and algorithms involved in implementing Distributed Shared Memory (DSM) in a Distributed Operating System. (CO4, K3)

Or

(b) Discuss the importance of security in Distributed Operating Systems (DOS) and explain the basic elements of Information System security and policy. (CO4, K3)

20. (a) Explain the process of configuring email, web services, NFS, and DNS on a Linux system. (CO5, K3)

Or

(b) How can you secure a Linux server using IP Tables and configure SSL certificates with OpenSSL? (CO5, K3)

————————

7 R2861

R2862

M.Sc. DEGREE EXAMINATION, APRIL – 2025

Second Semester

Cyber Forensics

PYTHON PROGRAMMING

(CBCS – 2023 onwards)

Time : 3 Hours   Maximum : 75 Marks

Part A   (10 × 1 = 10)

Answer **all** the objective questions by choosing the correct option.

1.   Which of the following is the correct syntax to declare a variable in Python?   (CO1, K1)

     (a)   variable = 10   (b)   10 = variable

     (c)   int variable = 10   (d)   var: int = 10

2.   Which of the following data types is immutable in Python?   (CO1, K1)

     (a)   List   (b)   Set

     (c)   Tuple   (d)   Dictionary

3.   Which Python module is commonly used for handling date and time operations?   (CO2, K1)

     (a)   time   (b)   datetime

     (c)   calendar   (d)   date

4. What will the following code output? (CO2, K1)

   import time

   print(time. sleep (2))

   (a) None   (b) 2

   (c) 2 seconds   (d) 2 seconds of pause

5. Which of the following is the correct mode for opening a file in Python for both reading and writing without truncating the file? (CO3, K1)

   (a) r+   (b) w+

   (c) a+   (d) r

6. Which method is used to write data to a file in Python? (CO3, K1)

   (a) write( )

   (b) writelines( )

   (c) Both (a) and (b)

   (d) None of the above

7. Which of the following methods can be used to create an iterator in Python? (CO4, K1)

   (a) _iter_( ) and _next_( )

   (b) iter( ) and next( )

   (c) _next_( ) and iter( )

   (d) All of the above

2   **R2862**

8. What is the primary difference between a generator and an iterator in Python? (CO4, K1)

   (a) Generators are always faster than iterator

   (b) Generators use yield to return values, while iterators use__next__( )

   (c) Generators are not iterable

   (d) Iterators cannot be used in loops

9. Which Python library is commonly used to interface with MySQL databases? (CO5, K1)

   (a) mysql   (b) MySQLdb

   (c) PyMySQL   (d) SQLite3

10. What does the rowcount attribute of a cursor in Python indicate after executing an SQL query? (CO5, K1)

    (a) The number of rows affected by the query

    (b) The number of rows selected

    (c) The total number of rows in the table

    (d) The number of errors encountered during the query

Part B (5 × 5 = 25)

Answer **all** the questions not more than 500 words each.

11. (a) Explain the difference between a list and a tuple in Python. (CO1, K2)

   Or

   (b) How does Python handle conditional statements? Explain with an example. (CO1, K2)

3   R2862

12. (a) Explain how the sleep( ) function in Python works and provide an example. (CO2, K2)

Or

(b) What is the role of the datetime module in Python, and how can it be used to manipulate date and time? (CO2, K2)

13. (a) Explain the difference between text files and binary files. How does Python handle them? (CO3, K2)

Or

(b) What are the different file opening modes in Python? Explain with examples. (CO3, K2)

14. (a) Explain what an iterator is in Python and how it works. Include an example of creating a custom iterator. (CO4, K2)

Or

(b) What is the purpose of yield in a Python generator, and how does it differ from return? Provide an example. (CO4, K2)

15. (a) Explain how to establish a connection to a MySQL database in Python. What are the necessary steps involved? (CO5, K2)

Or

(b) What is the purpose of a cursor in Python when working with MySQL? Explain with an example.
(CO5, K2)

R2862

Answer **all** the questions not more than 1,000 words each.

16. (a) Explain the concept of Python collections and compare the features of lists, tuples, sets, and dictionaries. (CO1, K3)

Or

(b) Analyze the importance loops Python programming. Provide examples of for and while loops. (CO1, K5)

17. (a) Analyze how Python's remodule can be used to validate an email address and explain the components of the regular expression used. (CO2, K5)

Or

(b) Evaluate the use of findall( ) and search( ) methods in Python's remodule with examples. (CO2, K5)

18. (a) Discuss how to work with CSV files in Python. How do you read and write data to a CSV file using Python? (CO3, K4)

Or

(b) Explain the process of working with binary files in Python. How do you read, write and close a binary file? (CO3, K2)

19. (a) Explain the concept of inheritance in Python. How does inheritance promote code reuse? Provide an example of both single and multiple inheritance. (CO4, K3)

Or

(b) Discuss polymorphism in Python. How is it implemented? Provide examples for method overriding and method overloading. (CO4, K3)

R2862

20. (a) How do you perform an UPDATE operation in MySQL using Python? Provide an example that updates a specific record based on a condition.

(CO5, K3)

Or

(b) Describe the process of creating a table in MySQL using Python. Explain the required steps and provide an example that creates a table with different data types. (CO5, K3)

————————

R2862

R2863

Sub. Code
556204

M.Sc. DEGREE EXAMINATION, APRIL – 2025

Second Semester

Cyber Forensics

ML FOR DIGITAL FORENSICS

(CBCS – 2023 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

Answer **all** the objective questions by choosing the correct option.

1. What is the primary motivation behind using Machine Learning techniques? (CO1, K2)

   (a) To reduce the time spent on manual computation

   (b) To enable systems to learn from data and improve their performance over time

   (c) To eliminate the need for any programming

   (d) To make systems capable of performing complex calculations

2. In supervised learning, the learning system is provided with which type of data? (CO1, K2)

   (a) Data without labels

   (b) Unlabeled data

   (c) Labeled data

   (d) Data without features

3. Which of the following methods is used for dimensionality reduction? (CO2, K2)

    (a) Principle Component Regression

    (b) Subset Selection

    (c) Linear Discriminant Analysis

    (d) All of the above

4. In Principal Component Regression (PCR), which technique is used to reduce the dimensionality before performing regression? (CO2, K2)

    (a) Ridge regression

    (b) Principal Component Analysis (PCA)

    (c) Lasso regression

    (d) Linear regression

5. Which of the following is a key feature of Naïve Bayes classifiers? (CO3, K2)

    (a) It assumes that features are dependent on each other

    (b) It assumes that features are independent given the class label

    (c) It is only applicable for continuous data

    (d) It uses decision trees as the classification model

6. Which distribution does Naïve Bayes use for continuous data in the Gaussian Naïve Bayes variant? (CO3, K2)

    (a) Bernoulli Distribution

    (b) Poisson Distribution

    (c) Gaussian Distribution

    (d) Multinomial Distribution

R2863

7. Which of the following is an early model of artificial neural networks? (CO4, K2)

   (a) Perceptron

   (b) Random Forest

   (c) Support Vector Machine

   (d) K-Nearest Neighbors

8. In the backpropagation algorithm, what is primarily updated during the training of a neural network? (CO4, K2)

   (a) Activation function

   (b) Network weights

   (c) Hyperparameters

   (d) Output layers

9. Which of the following is a common method used in malware detection? (CO5, K2)

   (a) Heuristic Analysis

   (b) Data Compression

   (c) IP Address Filtering

   (d) Quantum Key Distribution

10. In Network Intrusion Detection Systems (NIDS), which of the following is primarily used to identify unauthorized access or attacks? (CO5, K2)

    (a) Packet Sniffing   (b) Signature-based detection

    (c) Data Encryption   (d) Compression Algorithms

R2863

Part B $(5 \times 5 = 25)$

Answer **all** the questions not more than 500 words each.

11. (a) Explain the concept of well-posed learning problems. (CO1, K2)

    Or

    (b) Describe the importance of motivation in machine learning. (CO1, K3)

12. (a) Define and explain the concept of Subset Selection in dimensionality reduction. (CO2, K2)

    Or

    (b) What are Shrinkage methods, and how are they applied in regression models? (CO2, K2)

13. (a) Explain the concept of Supervised Learning and its applications. (CO3, K2)

    Or

    (b) Define and explain Unsupervised Learning with examples. (CO3, K2)

14. (a) Explain the concept of Backpropagation in Artificial Neural Networks. (CO4, K2)

    Or

    (b) Describe the role of Initialization in training artificial neural networks. (CO4, K3)

15. (a) Explain how heuristic analysis is used in malware detection. (CO5, K2)

    Or

    (b) Describe the difference between signature-based and anomaly- based detection in network intrusion detection systems. (CO5, K3)

4   R2863

Part C (5 × 8 = 40)

Answer **all** the questions not more than 1000 words each.

16. (a) Explain the types of machine learning and their key differences. (CO1, K3)

Or

   (b) Discuss the importance and challenges of Concept Learning in Machine Learning. (CO1, K3)

17. (a) Explain the steps and significance of Principal Component Analysis (PCA) in dimensionality reduction. (CO2, K3)

Or

   (b) Describe the difference between Ridge Regression and Lasso Regression. (CO2, K4)

18. (a) Discuss the differences between Hard Margin and Soft Margin Support Vector Machines. (CO3, K3)

Or

   (b) Explain the K-Means clustering algorithm and how it works. (CO3, K3)

19. (a) Analyze the advantages and disadvantages of using Backpropagation for training Artificial Neural Networks. (CO4, K5)

Or

   (b) Evaluate the importance of Ensemble Methods in improving machine learning model performance. (CO4, K5)

5

R2863

20. (a) Analyze the advantages and limitations of using signature-based detection in malware detection systems. (CO5, K5)

Or

(b) Evaluate the effectiveness anomaly-based intrusion detection systems (IDS) in modern networks. (CO5, K5)

————————

6 **R2863**

R2864		Sub. Code
		556206

M.Sc. DEGREE EXAMINATION, APRIL – 2025

Second Semester

Cyber Forensics

DIGITAL SIGNATURE

(CBCS – 2023 onwards)

Time : 3 Hours   Maximum : 75 Marks

Part A   (10 × 1 = 10)

Answer **all** the objective questions by choosing the correct options.

1. Which of the following is an example of symmetric encryption? (CO1, K1)

    (a) RSA   (b) AES

    (c) Diffie-Hellman   (d) ElGamal

2. Which cryptographic algorithm is based on the principle of two different keys for encryption and decryption? (CO1, K1)

    (a) Symmetric Encryption

    (b) Asymmetric Encryption

    (c) Hash Functions

    (d) XOR Encryption

3. Which of the following algorithms is commonly used for generating digital signatures? (CO2, K1)

    (a) RSA   (b) DES

    (c) SHA-1   (d) AES

4. What is the main function of a hash function in digital signatures? (CO2, K2)

   (a) To encrypt the message

   (b) To produce a fixed-length hash value from a variable-length message

   (c) To generate private keys

   (d) To decrypt the message

5. Which of the following is a primary function of a Certificate Authority (CA) in a PKI system? (CO3, K1)

   (a) To generate user passwords

   (b) To manage the private keys of users

   (c) To issue digital certificates

   (d) To encrypt data messages

6. What is the role of a Certificate Revocation List (CRL) in PKI? (CO3, K1)

   (a) It lists all valid certificates

   (b) It holds the public keys of users

   (c) It contains a list of revoked certificates

   (d) It stores certificates pending validation

7. Which of the following is a major challenge in digital signature forensics? (CO4, K1)

   (a) Lack of encryption algorithms

   (b) Loss of the private key used for signing

   (c) Insufficient bandwidth for certificate distribution

   (d) Lack of digital certificate authorities (CAs)

R2864

8. In the context of digital signature forensics, what is a potential problem when verifying the authenticity of a signature? (CO4, K1)

   (a) Signature encryption key mismatch

   (b) Signature timing discrepancy

   (c) Lack of a trusted Certificate Authority (CA)

   (d) All of the above

9. Which of the following is a key threat posed by quantum computing to classical digital signatures? (CO5, K1)

   (a) Increased computational time for signature verification

   (b) The possibility of breaking encryption schemes like RSA and ECC

   (c) Higher storage requirements for digital signatures

   (d) More accurate forensic analysis of blockchain transactions

10. Post-Quantum Cryptography (PQC) aims to: (CO5, K1)

   (a) Develop new encryption algorithms that are secure even against quantum computing attacks

   (b) Replace all existing digital signature algorithms

   (c) Use quantum computing for faster encryption and decryption

   (d) Reduce the storage size of digital signatures

R2864

Part B (5 × 5 = 25)

Answer **all** the questions not more than 500 words each.

11. (a) Explain the difference between symmetric and asymmetric encryption. (CO1, K2)

Or

(b) What is a hash function, and why is it important in cryptography? (CO1, K2)

12. (a) Explain the basic concept of a digital signature. How does it work to ensure message authenticity and integrity? (CO2, K2)

Or

(b) What is the difference between RSA and DSA in the context of digital signatures? (CO2, K2)

13. (a) Explain the basic concept of Public Key Infrastructure (PKI) and its role in ensuring secure communication. (CO3, K2)

Or

(b) What are the main components of a Public Key Infrastructure (PKI)? (CO3, K2)

14. (a) Explain the role of digital signatures in forensic investigations. (CO4, K2)

Or

(b) What are the common challenges faced when verifying digital signatures in a forensic investigation? (CO4, K2)

4 R2864

15. (a) Explain how quantum computing could potentially break classical encryption methods such as RSA and ECC. (CO5, K2)

Or

(b) Describe the role of Post-Quantum Cryptography in securing digital signatures against quantum attacks. (CO5, K3)

Part C (5 × 8 = 40)

Answer **all** the questions not more than 1000 words each.

16. (a) Explain the working of the AES (Advanced Encryption Standard) algorithm. (CO1, K3)

Or

(b) Discuss the RSA algorithm in detail, including key generation, encryption, and decryption. (CO1, K4)

17. (a) Discuss the RSA algorithm for digital signatures. Include the steps for key generation, signing, and verification. (CO2, K3)

Or

(b) Explain the working of the Digital Signature Algorithm (DSA) and compare it with RSA. (CO2, K3)

18. (a) Discuss the role of a Certificate Authority (CA) in PKI, detailing its functions and how it ensures trust in digital certificates. (CO3, K3)

Or

(b) Explain the key management process in PKI and its importance in ensuring the security of encrypted communications. (CO3, K3)

5

R2864

19. (a) Discuss the potential pitfalls in digital signature forensics and the challenges faced when validating digital signatures in a forensic context. (CO4, K4)

Or

(b) Describe the process of digital signature verification in forensic investigations, and explain how forensic analysts validate the integrity of a signed document. (CO4, K3)

20. (a) Analyse the potential impact of quantum computing on the security of digital signatures, particularly in the context of blockchain technology. (CO5, K5)

Or

(b) Evaluate the role of blockchain forensics in ensuring the accountability and traceability of transactions in the era of quantum computing. (CO5, K5)

————————

R2864

R2865

M.Sc. DEGREE EXAMINATION, APRIL – 2025

Second Semester

Cyber Forensics

Elective – WIRELESS NETWORK SECURITY

(CBCS – 2023 onwards)

Time : 3 Hours   Maximum : 75 Marks

Part A   (10 × 1 = 10)

Answer **all** the objective questions by choosing the correct option.

1. Which of the following is a primary goal of wireless network security? (CO1, K1)

    (a) To reduce signal interference

    (b) To prevent unauthorized access and ensure data integrity

    (c) To increase transmission speed

    (d) To enhance bandwidth utilization

2. Which of the following wireless security mechanisms helps prevent unauthorized interception of data? (CO1, K1)

    (a) Frequency Hopping Spread Spectrum (FHSS)

    (b) Active Threat Models

    (c) Cryptographic Hash Functions

    (d) Digital Signatures

3. Which of the following 802.11 standards supports a maximum data rate of 54 Mbps? (CO2, K1)

   (a) 802.11a   (b) 802.11b

   (c) 802.11g   (d) 802.11d

4. What is the primary security feature introduced by WPA (Wi-Fi Protected Access)? (CO2, K1)

   (a) Network Address Translation (NAT)

   (b) Temporal Key Integrity Protocol (TKIP)

   (c) Spread Spectrum technology

   (d) Frequency Hopping Spread Spectrum (FHSS)

5. Which of the following services is typically associated with GPRS (General Packet Radio Service)? (CO3, K1)

   (a) Voice call services

   (b) High-speed internet access

   (c) Short Message Service (SMS)

   (d) Email, services

6. Which mobile network technology supports the fastest data transfer rates among the following? (CO3, K1)

   (a) GSM   (b) UMTS

   (c) HSDPA   (d) GPRS

7. Which of the following is a key challenge in securing Wireless Sensor Networks (WSNs)? (CO4, K1)

   (a) Limited energy and computational resources

   (b) High data throughput

   (c) Centralized authentication

   (d) Unlimited bandwidth

R2865

8. In ZigBee security, which of the following is used for key establishment? (CO4, K1)

    (a) RSA

    (b) AES

    (c) Diffie-Hellman

    (d) ECC (Elliptic Curve Cryptography)

9. Which of the following ISO standards is specifically focused on Information Security Management Systems (ISMS)? (CO5, K1)

    (a) ISO/IEC 13335   (b) ISO/IEC 17799

    (c) ISO/IEC 27001   (d) ISO/IEC 9001

10. What is the primary purpose of a security policy in an organization? (CO5, K1)

    (a) To define the legal requirements for data retention

    (b) To outline the framework for managing security risks

    (c) To ensure that employees are aware of the company's holiday schedules

    (d) To limit physical access to the building

Part B   (5 × 5 = 25)

Answer **all** the questions not more than 500 words each.

11. (a) Explain the key objectives of wireless security. (CO1, K2)

                             Or

     (b) What is the role of cryptography in wireless network security? (CO1, K2)

R2865

12. (a) Explain the key differences between 802.11a and 802.11b standards. (CO2, K2)

Or

(b) What are the main security requirements for wireless networks, and how does WPA/WPA2 address them? (CO2, K2)

13. (a) Explain how GPRS (General Packet Radio Service) improves the efficiency of mobile data transmission compared to traditional GSM. (CO3, K2)

Or

(b) What are the key difference between SMS, EMS and MMS in terms of mobile messaging? (CO3, K2)

14. (a) Describe the main security threats faced by Wireless Sensor Networks(WSNs). (CO4, K3)

Or

(b) Explain the concept of key establishment and distribution in WSNs and its importance for network security. (CO4, K2)

15. (a) Explain the main components of a security policy and its importance in an organization. (CO5, K2)

Or

(b) Discuss the importance of ISO/IEC 27001 in establishing an Information Security Management System (ISMS). (CO5, K3)

4

R2865

Part C $(5 \times 8 = 40)$

Answer **all** the questions not more than 1000 words each.

16. (a) Analyse the impact of jamming attacks on wireless network security and discuss the effectiveness of anti-jamming techniques.   (CO1, K4)

Or

(b) Compare and contrast Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) in terms of their security features and applications.   (CO1, K4)

17. (a) Analyse the differences between WPA and WPA2 security protocols in wireless networks.   (CO2, K5)

Or

(b) Evaluate the security challenged associated with Wi-Fi networks and the role of WPA2 in mitigating these challenges.   (CO2, K5)

18. (a) Evaluate the security threats and protection measures for a mobile device when the attacker is in possession of the device.   (CO3, K5)

Or

(b) Analyze the potential security risks associated with the use of mobile networks like GSM, GPRS, and UMTS for data transmission.   (CO3, K4)

19. (a) Analyze the security challenges of Wireless Sensor Networks (WSNs) and evaluate the effectiveness of various cryptographic primitives used to secure these networks.   (CO4, K5)

Or

5   R2865

(b) Evaluate the security measures used in Near Field Communication (NFC) and RFID systems, and compare their vulnerabilities. (CO4, K5)

20. (a) Analyze the relationship between security policy, risk management, and ISO/IEC 27001 in ensuring organizational security. (CO5, K5)

Or

(b) Evaluate the role of ISO/IEC 17799 (now ISO/IEC 27002) in the development and implementation of security controls in an organization. (CO5, K5)

————————

R2865

R2866	Sub. Code
	556401

M.Sc. DEGREE EXAMINATION, APRIL – 2025

Second Semester

Cyber Forensics

REVERSE ENGINEERING AND MALWARE ANALYSIS

(CBCS – 2023 onwards)

Time : 3 Hours   Maximum : 75 Marks

Part A   (10 × 1 = 10)

Answer **all** the following objective questions by choosing the correct option.

1. What is the primary goal of reverse engineering in cybersecurity? (CO1, K1)

   (a) To create new malware

   (b) To analyze and understand malware behavior

   (c) To develop new programming languages

   (d) To improve software performance

2. Which tool is commonly used for static malware analysis? (CO1, K1)

   (a) Wireshark   (b) IDA Pro

   (c) Burp Suite   (d) SQLmap

3. What type of malware spreads by attaching itself to executable files? (CO2, K2)

   (a) Trojan Horse   (b) Worm

   (c) Virus   (d) Ransomware

4. Which phase of the malware lifecycle involves execution and payload activation? (CO2, K2)

   (a) Propagation

   (b) Infection

   (c) Execution

   (d) Encryption

5. What is the primary function of a Trojan Horse? (CO3, K1)

   (a) Self-replication

   (b) File encryption

   (c) Gaining unauthorized access

   (d) Sending spam emails

6. The Conficker C Worm is known for which type of attack? (CO3, K2)

   (a) Data wiping

   (b) Keylogging

   (c) Botnet formation

   (d) Ransomware encryption

7. What is the people of a concealer in a computer virus? (CO4, K2)

   (a) Encrypts the payload

   (b) Spreads the virus

   (c) Activates the virus

   (d) Deletes system files

2

R2866

8. Which programming language is commonly used for writing shell bash viruses? (CO4, K2)

   (a) Java   (b) Python

   (c) Bash   (d) C++

9. What is the first step in analyzing a malware specimen? (CO5, K2)

   (a) Execution on a live system

   (b) Establishing a controlled environment

   (c) Removing system logs

   (d) Disconnecting the internet

10. Which tool is commonly used for observing malware network activity? (CO5, K1)

   (a) IDA Pro

   (b) Process Monitor

   (c) Wireshark

   (d) OllyDbg

Part B (5 × 5 = 25)

Answer **all** the questions in not more than 500 words each.

11. (a) What is reverse engineering in cybersecurity? Explain its importance in malware analysis. (CO1, K2)

   Or

   (b) List and describe essential tools used in malware handling. (CO1, K3)

3   R2866

12. (a) Describe the key stages in a malware's lifecycle.

(CO2, K2)

Or

(b) Describe different types of malware. How does each type impact system security? (CO2, K2)

13. (a) Describe about Trojan Horse? Explain how it enables unauthorized access. (CO3, K2)

Or

(b) How is a covert channel implemented malware? Provide a real-world example. (CO3, K3)

14. (a) Explain the main components of a computer virus.

(CO4, K2)

Or

(b) What is polymorphic malware? How does it evade detection? (CO4, K3)

15. (a) Describe the key steps in analyzing a malware specimen. (CO5, K1)

Or

(b) Evaluate the role of system and network monitoring in detecting malware activity. (CO5, K3)

4 **R2866**

Part C $(5 \times 8 = 40)$

Answer **all** the questions in not more than 1000 words each.

16. (a) Explain the process of static and dynamic analysis in reverse engineering. How are they used to examine malware behaviour? (CO1, K2)

Or

(b) Evaluate the challenges faced while handling and analyzing malware in a secure lab environment. (CO1, K4)

17. (a) Discuss the characteristics and behaviour of different malware types such as viruses, worms, and ransomware. (CO2, K2)

Or

(b) Analyze the significance of signature-based and heuristic-based malware detection techniques. (CO2, K4)

18. (a) Describe the role of remote access tools in malware attacks. How do hackers use them to gain control of a system? (CO3, K3)

Or

(b) Critically analyze the working principle of logic bombs and their impact on cybersecurity. (CO3, K4)

19. (a) Compare and contrast metamorphic and polymorphic malware techniques. (CO4, K4)

Or

(b) Explain the different trigger mechanisms used in virus programming. How do they affect system performance? (CO4, K2)

5

R2866

20. (a) Illustrate the role of registry monitoring in malware detection. How does it help in forensic investigations? (CO5, K3)

Or

(b) Analyze the effectiveness of automated malware analysis frameworks. What are their limitations? (CO5, K4)

————————

R2866