R2085

Sub. Code
556101

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2024

First Semester

Cyber Forensics

INTRODUCTION TO CYBER FORENSICS

(CBCS – 2023 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

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

1. Which of the following is an example of cyber crime? (CO1, K1)

   (a) Theft of physical goods

   (b) Identity theft online

   (c) Cyber warfare

   (d) Network security audit

2. What is phishing? (CO1, K1)

   (a) Type of malware

   (b) Social engineering attack

   (c) Network vulnerability

   (d) Denial-of-Service (DoS) attack

3. Which category includes crimes like hacking and malware? (CO2, K1)

   (a) Cyber vandalism (b) Cyber theft

   (c) Cyber espionage (d) Cyber sabotage

4. What is the primary motivation behind most cyber crimes? (CO2, K1)

   (a) Financial gain (b) Political agendas

   (c) Personal revenge (d) Curiosity

5. Which database security measure prevents SQL injection attacks? (CO3, K1)

   (a) Firewalls

   (b) Intrusion Detection Systems

   (c) Input validation

   (d) Data masking

6. What is cyber forensics? (CO3, K1)

   (a) Investigating cyber crimes

   (b) Protecting networks from attacks

   (c) Recovering deleted data

   (d) Analyzing log files

7. What is the purpose of chain of custody in digital evidence handling? (CO4, K1)

   (a) Ensure evidence integrity

   (b) Document evidence transfer

   (c) Prevent evidence tampering

   (d) All of the above

8. What is the first step in digital evidence acquisition? (CO4, K1)

   (a) Collection (b) Preservation

   (c) Identification (d) Analysis

9. In the case of Sony Pictures Entertainment hack (2014), what type of malware was used? (CO5, K1)

   (a) Ransomware (b) Wiper malware

   (c) Spyware (d) Trojan

10. Which cybercrime case involved the theft of over 147 million credit card numbers? (CO5, K1)

   (a) Target breach (2013)

   (b) Heartland Payment Systems breach (2008)

   (c) TJX Companies breach (2006-2007)

   (d) Equifax breach (2017)

Part B (5 × 5 = 25)

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

11. (a) List four types of cyber crimes that affect individuals. (CO1, K4)

Or

(b) Explain the term 'malware' and its impact on network security. (CO1, K4)

12. (a) Explain the difference between cyber theft and cyber fraud. (CO2, K3)

Or

(b) Describe cyber espionage and its significance. (CO2, K5)

13. (a) Explain the importance of access control in database security. (CO3, K3)

Or

(b) Explain the concept of digital evidence and its types. (CO3, K5)

14. (a) Explain the importance of identification in digital evidence acquisition. (CO4, K5)

Or

(b) Describe the goal and scope of digital evidence analysis. (CO4, K4)

15. (a) Explain the role of authentication in establishing the admissibility of digital evidence. (CO5, K5)

Or

(b) Describe the modus operandi of the hacker group "Anonymous" and its implications for cyber security. (CO5, K3)

Part C (5 × 8 = 40)

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

16. (a) Discuss the role of network security in preventing cyber crimes. (CO1, K5)

Or

(b) Explain the concept of malware and its impact on network security. (CO1, K5)

17. (a) Explain the concept of cyber espionage and its significance in today's digital landscape. Provide two examples. (CO2, K5)

Or

(b) Explain the concept of cyber warfare and its significance in international relations. (CO2, K5)

18. (a) Explain the concept of database security and its significance in protecting sensitive data. (CO3, K5)

Or

(b) Describe the cyber forensics process and its role in investigating cyber crimes. (CO3, K4)

19. (a) Compare and contrast computer, network, and mobile forensic analysis. (CO4, K5)

Or

(b) Explain the concept of timeline analysis in digital evidence analysis. (CO4, K4)

20. (a) Critically evaluate the importance of digital evidence authentication in ensuring its admissibility in court. (CO5, K4)

Or

(b) Discuss the role of digital forensics in investigating and prosecuting cybercrime, using a notable case study. (CO5, K4)

———————

R2086

Sub. Code
556102

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2024

First Semester

Cyber Forensics

CYBER CRIME ISSUES AND INVESTIGATION

(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 type of cybercrime involves unauthorized access to computer systems or networks? (CO1, K1)

   (a) Phishing

   (b) Hacking

   (c) Malware

   (d) Identity Theft

2. Which international treaty addresses cybercrime? (CO1, K1)

   (a) Budapest Convention

   (b) Geneva Convention

   (c) Hague Convention

   (d) EU Directive

3. What is the primary goal of preparing a cybercrime case for prosecution? (CO2, K1)

   (a) To gather evidence

   (b) To identify suspects

   (c) To establish probable cause

   (d) To secure a conviction

4. What is the purpose of direct examination in a cybercrime trial? (CO2, K1)

   (a) To challenge the witness's credibility

   (b) To present evidence

   (c) To cross-examine the witness

   (d) To establish the witness's expertise

5. Which incident response phase involves identifying and assessing the scope of the incident? (CO3, K1)

   (a) Containment (b) Eradication

   (c) Recovery (d) Identification

6. What WiFi encryption protocol is most vulnerable to interception? (CO3, K1)

   (a) WPA2 (b) WPA

   (c) WEP (d) Open

7. Which investigative technique involves monitoring network traffic? (CO4, K1)

   (a) Network forensics

   (b) Digital forensics

   (c) Mobile forensics

   (d) Surveillance

8. How should mobile devices be handled during investigation? (C04, K1)

(a) Powered on and analyzed immediately

(b) Powered off and stored securely

(c) Accessed remotely

(d) Shared with third parties

9. Which tool is commonly used for network traffic analysis? (CO5, K1)

(a) Wireshark (b) EnCase

(c) FTK (d) Volatility

10. What investigative technique involves analyzing financial transactions? (CO5, K1)

(a) Forensic accounting

(b) Digital forensics

(c) Network analysis

(d) Social network analysis

Part B (5 × 5 = 25)

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

11. (a) Explain the concept of phishing and its impact on computer security. (CO1, K4)

Or

(b) Explain the significance of the computer Fraud and Abuse Act (CFAA) in combating computer crime. (CO1, K4)

12. (a) Explain the importance of documenting electronic evidence in cybercrime investigations. (CO2, K4)

Or

(b) Describe the key elements of effective expert testimony in cybercrime trials. (CO2, K5)

13. (a) Explain the importance of incident containment in incident response. (CO3, K3)

Or

(b) Explain the differences between live forensics and post-mortem analysis. (CO3, K5)

14. (a) Explain the importance of documenting electronic evidence in cybercrime investigations. (CO4, K4)

Or

(b) Explain the differences between logical and physical acquisition in mobile forensics. (CO4, K4)

15. (a) Explain the role of forensic accounting in investigating financial frauds. (CO5, K4)

Or

(b) Explain the importance of incident response planning in investigating cybercrimes, using the Equifax breach as a case study. (CO5, K4)

Part C (5 × 8 = 40)

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

16. (a) Critically evaluate the impact of phishing attacks on individuals and organizations, discussing prevention strategies. (CO1, K5)

Or

(b) Compare and contrast hacking and cracking, discussing motivations and consequences. (CO1, K5)

17. (a) Discuss the role of search warrants in cybercrime investigations, highlighting requirements and limitations (CO2, K5)

Or

(b) Compare and contrast the' rules of evidence for digital and physical evidence in cybercrime investigations. (CO2, K5)

18. (a) Critically evaluate the importance of incident containment and eradication in preventing further damage. (CO3, K5)

Or

(b) Explain the differences between wiretapping and interception in the context of WiFi transmissions, discussing legal and technical distinctions. (CO3, K4)

19. (a) Critically evaluate the importance of incident response planning in cybercrime investigations. (CO4, K5)

Or

(b) Describe the process of conducting a GPS location tracking analysis in mobile forensic investigations. (CO4, K4)

20. (a) Critically evaluate the role of auditing in preventing and detecting financial fraud, using the Enron scandal as a case study. (CO5, K4)

Or

(b) Explain the importance of threat intelligence in investigating and preventing cybercrimes, using the WannaCry ransomware attack as a case study. (CO5, K4)

———————

R2087

Sub. Code
556103

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2024

First Semester

Cyber Forensics

ADVANCED DATABASE SECURITY

(CBCS – 2023 onwards)

Time : Three Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

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

1. Which of the following is a method to ensure data confidentiality in a database? (CO1, K1)

   (a) Data Redundancy

   (b) Encryption

   (c) Indexing

   (d) Normalization

2. What is the primary purpose of database auditing? (CO1, K1)

   (a) To enhance performance

   (b) To track changes and access to data

   (c) To optimize queries

   (d) To manage data storage

3. Which access control model is based on the concept of roles assigned to users? (CO2, K1)

   (a) Discretionary Access Control

   (b) Mandatory Access Control

   (c) Role-Based Access Control

   (d) Attribute-Based Access Control

4. What technique can be employed to protect sensitive data in a database while still allowing certain queries? (CO2, K1)

   (a) Data Masking

   (b) Data Migration

   (c) Data Warehousing

   (d) Data Fragmentation

5. Which of the following threats involves an unauthorized user attempting to gain access to a database through exploiting vulnerabilities? (CO3, K1)

   (a) SQL Injection

   (b) Data Breach

   (c) Phishing

   (d) Denial of Service

6. What is the purpose of database encryption at rest? (CO3, K1)

   (a) To secure data in transit

   (b) To protect stored data from unauthorized access

   (c) To improve database performance

   (d) To ensure data integrity

7. Which of the following is NOT a common database security best practice? (CO4, K1)

   (a) Regularly updating database software

   (b) Using complex and unique passwords

   (c) Allowing public access to the database

   (d) Implementing strong access controls

8. What does the principle of least privilege advocate for? (CO4, K1)

   (a) Users should have access to all data

   (b) Users should have the minimum level of access required to perform their job

   (c) Users should have unrestricted access to the database

   (d) Users should be granted access based on seniority

9. Which type of attack aims to disrupt the availability of a database service? (CO5, K1)

   (a) Man-in-the-Middle Attack

   (b) Denial of Service (DoS) Attack

   (c) SQL Injection

   (d) Phishing Attack

10. What is the function of a Web Application Firewall (WAF) in relation to database security? (CO5, K1)

   (a) To enhance database performance

   (b) To filter and monitor HTTP requests to prevent SQL injection and other attacks

   (c) To encrypt database connections

   (d) To manage user authentication

Part B (5 × 5 = 25)

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

11. (a) Explain about Risk analysis. (CO1, K2)

Or

(b) Explain in detail about digital identification. (CO1, K2)

12. (a) Briefly explain about web server security. (CO2, K1)

Or

(b) Write a note on web application proxies. (CO2, K1)

13. (a) Explain access control models in XML in detail. (CO3, K4)

Or

(b) Write a note on security in data warehouses. (CO3, K4)

14. (a) Explain about trustworthy records retention. (CO4, K3)

Or

(b) Write a note on damage quarantine. (CO4, K3)

15. (a) Explain privacy – enhanced location. (CO5, K5)

Or

(b) Explain about privacy policy in a mobile environment. (CO5, K5)

Part C (5 × 8 = 40)

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

16. (a) Explain about working cryptographic system and protocols. (CO1, K2)

Or

(b) Explain legal restriction on cryptography. (CO1, K2)

17. (a) Explain about privacy – protecting techniques. (CO2, K1)

Or

(b) Explain the following (CO2, K1)

(i) Whois

(ii) Netcraft

(iii) Finger printing

18. (a) Explain OLAP systems in detail. (CO3, K4)

Or

(b) Explain about integrity controls in detail. (CO3, K4)

19. (a) Write a note an security re-engineering for database concept. (CO4, K3)

Or

(b) Explain database watermarking for copyright protection. (CO4, K3)

20. (a) Write a note on Bayesian perspective. (CO5, K5)

Or

(b) Explain about privacy – enhanced location in detail. (CO5, K5)

———————

R2088

Sub. Code
556104

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2024

First Semester

Cyber Forensics

CRYPTOGRAPHY AND NETWORK SECURITY

(CBCS – 2023 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

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

1. What is the primary purpose of cryptography? (CO1, K1)

   (a) Data compression

   (b) Data integrity

   (c) Data confidentiality

   (d) Data redundancy

2. Which of the following algorithms is NOT a symmetric key algorithm? (CO1, K1)

   (a) AES (b) DES

   (c) RSA (d) Blowfish

3. What type of attack involves intercepting and altering communications between two parties without their knowledge? (CO2, K1)

   (a) Replay attack

   (b) Man-in-the-middle attack

   (c) Denial of Service attack

   (d) Phishing attack

4. Which protocol is primarily used for secure communication over a computer network? (CO2, K1)

(a) HTTP (b) FTP

(c) HTTPS (d) SMTP

5. In which cryptographic technique is the same key used for both encryption and decryption? (CO3, K1)

(a) Asymmetric cryptography

(b) Symmetric cryptography

(c) Hashing

(d) Digital Signatures

6. What is a digital signature? (CO3, K1)

(a) A type of encryption

(b) A mechanism to ensure data integrity and authenticity

(c) A random number used in cryptographic processes

(d) A method for creating backups

7. Which of the following is a characteristic of asymmetric encryption? (CO4, K1)

(a) Same key for encryption and decryption

(b) Uses a pair of keys (public and private)

(c) Faster than symmetric encryption

(d) Less secure than symmetric encryption

8. What does SSL stand for? (CO4, K1)

(a) Secure Socket Layer

(b) Secure System Layer

(c) Simple Socket Layer

(d) System Security Layer

9. Which of the following is an example of a hashing algorithm? (CO5, K1)

(a) RSA (b) AES

(c) SHA-256 (d) DES

10. What does the term 'key exchange' refer to in cryptography? (CO5, K1)

(a) The process of sharing a symmetric key

(b) The process of creating a public key

(c) The process of deleting a key

(d) The process of encrypting data

Part B (5 × 5 = 25)

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

11. (a) Explain about security services. (CO1, K2)

Or

(b) Explain DES and Triple AES. (CO1, K2)

12. (a) Briefly explain about RSA algorithm. (CO2, K4)

Or

(b) Write a note on digital signature. (CO2, K3)

13. (a) Explain Kerberos in detail. (CO3, K4)

Or

(b) Write a note on email security. (CO3, K4)

14. (a) Explain about secure socket layer. (CO4, K4)

Or

(b) Write a note on Firewalls. (CO4, K3)

15. (a) Explain security audit. (CO5, K4)

Or

(b) Explain water marking in detail. (CO5, K4)

Part C (5 × 8 = 40)

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

16. (a) Explain symmetric and asymmetric key cryptosystem. (CO1, K4)

Or

(b) Explain stream cipher and block cipher algorithm. (CO1, K4)

17. (a) Explain about Hash and MAC algorithm. (CO2, K4)

Or

(b) Explain Diffie – Hellman key exchange in detail. (CO2, K4)

18. (a) Explain about encryption techniques in detail. (CO3, K4)

Or

(b) Explain the following: (CO3, K4)

(i) PGP – S

(ii) MIME

19. (a) Write a note an intruders and viruses. (CO4, K3)

Or

(b) Explain password security in detail. (CO4, K4)

20. (a) Write a note RSA algorithm. (CO5, K5)

Or

(b) Explain about DNA Cryptography. (CO5, K4)

———————

R2089

Sub. Code

556105

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2024

First Semester

Cyber Forensics

INFORMATION AND WEB SECURITY

(CBCS – 2023 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

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

1. Which of the following is considered the primary goal of information security? (CO1, K1)

   (a) Confidentiality

   (b) Availability

   (c) Integrity

   (d) All of the above

2. What does the principle of least privilege refer to? (CO1, K1)

   (a) Giving users only the access they need

   (b) Allowing all users full access

   (c) Restricting access to the system

   (d) None of the above

3. Which type of attack involves overwhelming a system with traffic to render it unusable? (CO2, K1)

   (a) Phishing

   (b) Denial of Service (DoS)

   (c) Man-in-the-Middle

   (d) Spoofing

4. What type of malware is designed to replicate itself and spread to other computers? (CO2, K1)

   (a) Virus (b) Worm

   (c) Trojan (d) Ransomware

5. What is the main purpose of a security operations center (SOC)? (CO3, K1)

   (a) To develop software

   (b) To monitor and respond to security incidents

   (c) To perform audits

   (d) To manage human resources

6. Which of the following is essential for incident response planning? (CO3, K1)

   (a) Regular system updates

   (b) A well-defined incident response team

   (c) Software firewalls only

   (d) User training programs

7. What is the primary purpose of HTTPS? (CO4, K1)

(a) Faster page load times

(b) Secure data transmission

(c) Improved SEO ranking

(d) User tracking

8. Which of the following is a common web security vulnerability? (CO4, K1)

(a) XSS (Cross-Site Scripting)

(b) SQL Injection

(c) CSRF (Cross-Site Request Forgery)

(d) All of the above

9. What is the primary purpose of data encryption in web privacy? (CO5, K1)

(a) To enhance website speed

(b) To protect user data from unauthorized access

(c) To improve user experience

(d) To track user behaviour

10. Which regulation primarily governs data protection and privacy in the European Union? (CO5, K1)

(a) HIPAA

(b) GDPR

(c) CCPA

(d) PCI DSS

Part B (5 × 5 = 25)

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

11. (a) Explain the implementation of the Secure Session Management Pattern in web applications. (CO1, K4)

Or

(b) Discuss the advantages of using the Security Filter Pattern in a multi-tier architecture. (CO1, K3)

12. (a) Explain the steps involved in a typical SQL injection attack and how to prevent it. (CO2, K4)

Or

(b) What are the key differences between a DoS and a DDoS attack. (CO2, K3)

13. (a) What is the role of configuration management in security? (CO3, K3)

Or

(b) Discuss the implications of security compliance frameworks. (CO3, K3)

14. (a) Discuss the implications of a data breach on a web application. (CO4, K3)

Or

(b) Explain the importance of regular security testing for websites. (CO4, K4)

15. (a) Describe the role of cookies in web tracking and methods to manage them. (CO5, K4)

Or

(b) Explain how a web application proxy integrates with a web application firewall. (CO5, K4)

Part C (5 × 8 = 40)

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

16. (a) What are the most significant vulnerabilities in today's cyber security frameworks and how can they be addressed? (CO1, K4)

Or

(b) What are the fundamental principles of information security, and how do they apply across different domains? (CO1, K4)

17. (a) What are the most effective strategies for preventing cyber attacks on critical infrastructure. (CO2, K4)

Or

(b) How does the rise of artificial intelligence impact the landscape of malicious attacks? (CO2, K3)

18. (a) How can organizations ensure effective communication and collaboration between security operations and other IT functions? (CO3, K3)

Or

(b) What role does automation play in maintaining secure configurations across diverse IT environments? (CO3, K3)

19. (a) What are the most effective cryptographic techniques for ensuring data integrity and confidentiality in web applications? (CO4, K4)

Or

(b) How do differing regulatory requirements across regions affect the implementation of cryptographic practices in web security? (CO4, K3)

20. (a) How does the use of web application proxies affect the effectiveness of privacy-preserving technologies like VPNs and Tor. (CO5, K3)

Or

(b) What are the future trends in web privacy that could impact the design and function of web application proxies? (CO5, K4)

R2090

Sub. Code
556501

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2024

First Semester

Cyber Forensics

Elective – FRAUDS AND COUNTER MEASURES

(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. Which of the following is considered a common indicator of financial fraud? (CO1, K1)

   (a) Consistent revenue growth

   (b) Frequent changes in accounting personnel

   (c) Strong internal controls

   (d) Transparent financial reporting

2. What is the primary purpose of financial accounting? (CO1, K1)

   (a) To prepare tax returns

   (b) To provide information for internal management decisions

   (c) To provide financial information to external stakeholders

   (d) To enhance marketing strategies

3. Which of the following is NOT a form of business entity? (CO2, K1)

   (a) Sole proprietorship

   (b) Partnership

   (c) Corporation

   (d) Bureaucracy

4. In financial analysis, what does liquidity refer to? (CO2, K1)

   (a) The ability to pay long-term debts

   (b) The ability to convert assets into cash quickly

   (c) The total revenue generated by a company

   (d) The profitability of a business over time

5. Which of the following factors is most likely to contribute to an organization's vulnerability to fraud? (CO3, K1)

   (a) Strong ethical culture

   (b) Lack of internal controls

   (c) Regular audits

   (d) Employee training programs

6. What psychological factor can make individuals more susceptible to committing fraud? (CO3, K1)

   (a) High self-esteem

   (b) Fear of failure

   (c) Strong ethical standards

   (d) Healthy work-life balance

7. What is often a key characteristic of a fraudster's mindset? (CO4, K1)

(a) High level of transparency

(b) Inability to recognize consequences

(c) Strong ethical values

(d) Focus on teamwork

8. In analyzing fraud cases, which motivation is commonly identified among fraudsters? (CO4, K1)

(a) Desire for personal fulfilment

(b) Greed and financial pressure

(c) Commitment to company success

(d) Need for recognition

9. What is the primary goal of evidence collection in fraud investigations? (CO5, K1)

(a) To enhance company reputation

(b) To gather sufficient proof for legal action

(c) To identify all employees involved

(d) To reduce costs

10. Which of the following is a crucial step in preserving evidence for legal proceedings? (CO5, K1)

(a) Sharing findings with all employees

(b) Documenting the chain of custody

(c) Discarding irrelevant information

(d) Making copies of evidence for personal use

Part B (5 × 5 = 25)

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

11. (a) Define financial accounting and explain its importance in detecting fraud. (CO1, K3)

Or

(b) Discuss the common types of financial fraud that organizations face today. (CO1, K4)

12. (a) What are the main differences between a sole proprietorship and a corporation? Discuss the implications for liability and taxation. (CO2, K3)

Or

(b) Explain the concept of financial analysis and its significance in assessing the performance of different business entities. (CO2, K4)

13. (a) Identify and explain three key factors that contribute to an organization's vulnerability to fraud. (CO3, K3)

Or

(b) Discuss the role of employee behavior and corporate culture in influencing vulnerability to fraud. (CO3, K4)

14. (a) Choose a well-known fraud case and summarize the key motivations behind the fraudster's actions. (CO4, K4)

Or

(b) What are the common psychological traits fraudsters and how do these traits influence their decision-making? (CO4, K3)

15. (a) What is the significance of chain of custody in the context of evidence collection? Discuss its role in legal proceedings. (CO5, K3)

Or

(b) List and explain the steps involved in the process of collecting evidence during a fraud investigation. (CO5, K4)

Part C (5 × 8 = 40)

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

16. (a) Analyze the role of internal controls in preventing financial fraud. Provide examples of effective internal control measures. (CO1, K5)

Or

(b) Evaluate how the ethical culture of an organization influences its vulnerability to financial fraud. Discuss ways to foster a strong ethical environment. (CO1, K5)

17. (a) Discuss the various financial ratios used in financial analysis. How can these ratios help stakeholders make informed decisions? (CO2, K4)

Or

(b) Evaluate the advantages and disadvantages of different forms of business entities in terms of investment and growth potential. (CO2, K4)

18. (a) Analyze the impact of economic conditions on an organization's susceptibility to fraud. Provide examples of how economic downturns can lead to increased fraud risks. (CO3, K5)

Or

(b) Examine the psychological factors that may drive individuals to commit fraud within an organization. How can organizations mitigate these risks? (CO3, K5)

19. (a) Conduct a detailed analysis of a specific case study of fraud. Discuss the methods used by the fraudster and the impact on the organization. (CO4, K5)

Or

(b) Evaluate the lessons learned from examining the mindset of fraudsters. How can these lessons be applied to prevent future fraud in organizations? (CO4, K5)

20. (a) Analyze the challenges faced in the collection and preservation of evidence in fraud cases. How can these challenges be effectively addressed? (CO5, K5)

Or

(b) Discuss the legal implications of mishandling evidence in fraud investigations. Provide examples of how this can affect legal outcomes. (CO5, K4)

———————

R2091

Sub. Code
556301

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2024

Third Semester

Cyber Forensics

ETHICAL HACKING

(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. ————— is the technique used in business organizations and firms to protect IT assets. (CO1, K2)

   (a) Ethical hacking (b) Unethical Hacking

   (c) Fixing Bugs (d) Internal data – breach

2. At which layer of the OSI communication model does bridge operate? (CO1, K2)

   (a) Network (b) Physical

   (c) Transport (d) Datalink

3. ————— is a component of the reconnaissance stage that is use to gather possible information for a target computer system or network. (CO2, K1)

   (a) Finger Printing (b) 3D Printing

   (c) Foot Printing (d) Data Printing

4. Spywares can be used to steal ————— from the attacker's browser. (CO2, K2)

   (a) Browser history (b) Company details

   (c) Plug-ins used (d) Browser details

5. ———————— type of exploit requires accessing to any vulnerable system for enhancing privilege for an attacker to run the exploit. (CO3, K1)

(a) Local exploits (b) Remote exploits

(c) System exploits (d) Network exploits

6. Windows server 2003 and 2008 ———————— are used to authenticate user accounts, so they contain much of the information that attackers want to access. (CO3, K1)

(a) SMB controllers (b) Domain controllers

(c) CIFS servers (d) File servers

7. In system hacking, which of the following is the most crucial activity? (CO4, K2)

(a) Information gathering

(b) Covering tracks

(c) Cracking passwords

(d) None of the above

8. In Wi-Fi Security, which of the following protocol is more used? (CO4, K2)

(a) WPA (b) WPA2

(c) WPS (d) Both (a) and (c)

9. What is the primary function of a firewall ———————— (CO5, K1)

(a) To detect and remove viruses

(b) To encrypt network traffic

(c) To control incoming and outgoing network traffic

(d) To provide network authentication

10. Which network protection system provides secure remote access to a network ————————. (CO5, K2)

(a) VPN (b) Firewall

(c) IDS (d) IPS

Part B (5 × 5 = 25)

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

11. (a) Explain the Ethical Hacking Terminology with suitable examples. (CO1, K5)

Or

(b) Explain the Internet layer. (CO1, K5)

12. (a) Examine why do attackers need foot printing. What are the objectives of foot printing? (CO2, K2)

Or

(b) Discuss about Scanning tools. (CO2, K4)

13. (a) Identify the counter measures against SMTP, LDAP and SMB enumeration. Explain. (CO3, K3)

Or

(b) Discuss about Vulnerability research. (CO3, K4)

14. (a) Demonstrate the web application vulnerability stack. (CO4, K5)

Or

(b) Explain the different wireless security layers. (CO4, K5)

15. (a) Explain firewall. (CO5, K5)

Or

(b) Explain about network based IDSs and IPSs (CO5, K5)

Part C (5 × 8 = 40)

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

16. (a) Explain the application layer. (CO1, K5)

Or

(b) Discuss the addressing physical security. (CO1, K4)

17. (a) State how the foot printing is done through social engineering? Explain. (CO2, K4)

Or

(b) Discuss in detail about scanning techniques. (CO2, K4)

18. (a) Elaborately discuss about NetBIOS. (CO3, K5)

Or

(b) Discuss in detail about vulnerabilities of OS. (CO3, K4)

19. (a) Elaborately discuss about Hacking Web Servers. (CO4, K4)

Or

(b) Discuss about Wireless Hacking. (CO4, K4)

20. (a) Discuss the CISCO adaptive security. (CO5, K4)

Or

(b) Explain Web filtering. (CO5, K5)

———————

R2092

Sub. Code
556302

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2024

Third Semester

Cyber Forensics

BEHAVIOURAL BIOMETRICS

(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. Who is father of biometrics ————— (CO1, K2)

   (a) Bernard Spilsbury

   (b) Sir Francis Galton

   (c) Aplphonse Bertillon

   (d) Henry fauls

2. Which biometric modality typically has a higher False Match Rate (FMR) compared to others? (CO1, K1)

   (a) Fingerprint recognition

   (b) Facial recognition

   (c) Iris scanning

   (d) Signature recognition

3. What is an expression in the context of speech recognition? (CO2, K1)

   (a) A sequence of words

   (b) A sequence of phonemes

   (c) A sequence of syllables

   (d) A sequence of gestures

4. Which of the following is a key aspect of computational phonology? (CO2, K1)

(a) Acoustic modeling

(b) Phonetic transcription

(c) Phonological rule-based modeling

(d) Language modeling

5. Which of the following is a key challenge in speech parsing? (CO3, K1)

(a) Dealing with accents and dialects

(b) Dealing with background noise

(c) Dealing with out-of-vocabulary words

(d) Dealing with syntactic ambiguity

6. Which of the following is a key aspect of computational lexical semantics? (CO3, K1)

(a) Word sense induction

(b) Word sense disambiguation

(c) Word sense representation

(d) All of the above

7. ——————— is gait kinematics? (CO4, K1)

(a) The study of gait movement patterns

(b) The study of gait force patterns

(c) The study of gait muscle activity

(d) The study of gait energy expenditure

8. ——————— EMG measure? (CO4, K1)

(a) Muscle activity (b) Nerve activity

(c) Brain activity (d) Heart activity

9. What happens to the whole-body center of mass during normal gait? (CO5, K1)

   (a) It remains stationary

   (b) It moves up and down

   (c) It moves forward and backward

   (d) It moves in a sinusoidal pattern

10. What is the primary application of competing voice scan technologies? (CO5, K1)

   (a) Security and surveillance

   (b) Healthcare and medical diagnosis

   (c) Marketing and advertising

   (d) Gaming and entertainment

Part B (5 × 5 = 25)

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

11. (a) Discuss in detail about benefits of biometric security. (CO1, K4)

Or

   (b) Explain Failure to enroll rate. (CO1, K5)

12. (a) Discuss about regular expressions. (CO2, K4)

Or

   (b) Explain about automatic speech recognition. (CO2, K5)

13. (a) Discuss about syntactic parsing. (CO3, K4)

Or

   (b) Explain the computational discourse. (CO3, K5)

14. (a) Define Gait Analysis. Explain it. (CO4, K4)

Or

(b) Illustrate Motion analysis. (CO4, K4)

15. (a) Discuss about Knee Joint. (CO5, K4)

Or

(b) Explain the Components operation in normal gait. (CO5, K5)

Part C (5 × 8 = 40)

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

16. (a) Briefly explain about basic working of biometric matching. (CO1, K5)

Or

(b) Explain Layered biometric solutions. (CO1, K5)

17. (a) Explain the Hidden Markov and entropy models. (CO2, K5)

Or

(b) Explain computational phonology. (CO2, K5)

18. (a) Explain the statistical parsing. (CO3, K5)

Or

(b) Discuss in detail about computational semantics. (CO3, K4)

19. (a) Elaborately discuss the fundamentals of Gait Analysis. (CO4, K4)

Or

(b) Explain about EMG. (CO4, K3)

20. (a) Discuss the Ankle and Foot complex. (CO5, K4)

Or

(b) Discuss about the strength and weakness of normal gait. (CO5, K4)

———————

R2093

Sub. Code
556305

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2024

Third Semester

Cyber Forensics

CYBER LAW POLICIES AND IT ACT

(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 legal issue in cyber space? (CO1, K1)

   (a) Intellectual property rights

   (b) Data privacy

   (c) Cybercrime

   (d) Jurisdiction

2. Which section of the IT Act 2000 deals with data protection? (CO1, K1)

   (a) Section 43A (b) Section 45

   (c) Section 66 (d) Section 72

3. What is the validity period of a DSC? (CO2, K1)

   (a) 1 year (b) 2 years

   (c) 3 years (d) 5 years

4. What is the primary motive behind most cyber crimes? (CO2, K1)

   (a) Revenge (b) Curiosity

   (c) Financial gain (d) Political activism

5. Which of the following is a type of cyber attack that can affect industrial control systems? (CO3, K1)

(a) Malware (b) Virus

(c) Trojan (d) Ransomware

6. Under Indian Evidence Law, which section deals with electronic evidence related to DoS attacks? (CO3, K1)

(a) Section 65A (b) Section 65B

(c) Section 79 (d) Section 85

7. What is the duration of copyright protection in India? (CO4, K1)

(a) 50 years from publication

(b) 60 years from publication

(c) 70 years from publication

(d) Lifetime of the author + 60 years

8. What is the benefit of using Creative Commons licenses in multimedia works? (CO4, K1)

(a) Waives all copyright rights

(b) Allows for flexible permissions

(c) Requires attribution and share–alike

(d) Prohibits commercial use

9. What is patent infringement? (CO5, K1)

(a) The act of applying for a patent

(b) The act of granting a patent

(c) The act of using someone else's patented invention without permission

(d) The act of abandoning a patent application

10. What is a domain name dispute? (CO5, K1)

(a) A conflict between two parties over a patent

(b) A conflict between two parties over a trademark

(c) A conflict between two parties over a domain name

(d) A conflict between two parties over a copyrights

Part B (5× 5 = 25)

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

11. (a) Discuss in detail about fundamentals of cyber space. (CO1, K4)

Or

(b) Discuss the overview of the act (CO1, K4)

12. (a) Discuss about Digital Signature Certificates (CO2, K4)

Or

(b) Explain about different kinds of cyber crimes. (CO2, K5)

13. (a) Discuss about cybercrime IT Act 2000 (CO3, K4)

Or

(b) Explain the data protection and privacy. (CO3, K5)

14. (a) Illustrate Copy rights. (CO4, K4)

Or

(b) Discuss about trademarks in Internet (CO4, K4)

15. (a) Discuss about understanding the patents. (CO5, K4)

Or

(b) Define Case laws. Explain it. (CO5, K5)

Part C (5 × 8 = 40)

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

16. (a) Briefly explain about interface of technology law (CO1, K5)

Or

(b) Explain the Aims and objects of IT Act 2000 (CO1, K5)

17. (a) Explain the legal recognition of electronic records and evidence. (CO2, K5)

Or

(b) Discuss about cybercrime under IPC (CO2, K4)

18. (a) Explain the cyber stalking. (CO3, K5)

Or

(b) Discuss in detail about cyber terrorism violation of privacy on Internet (CO3, K4)

19. (a) Elaborately discuss about the copyrights in internet (CO4, K4)

Or

(b) Discuss about copyright and trademark cases (CO4, K4)

20. (a) Discuss about Indian position on patents (CO5, K4)

Or

(b) Discuss about the IPR cases (CO5, K4)

R2094

Sub. Code
556306

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2024

Third Semester

Cyber Forensics

SOCIAL MEDIA FORENSICS

(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. Which of the following tools is used for social media forensic analysis? (CO1, K1)

    (a) Maltego   (b) Hootsuite

    (c) Buffer   (d) Sprout Social

2. Which of the following is an example of a social media cybercrime? (CO1, K1)

    (a) Posting a status update

    (b) Sharing a photo

    (c) Sending a friend request to a minor

    (d) Tagging a friend in a post

3. Which of the following is an example of information privacy disclosure in social media? (CO2, K1)

    (a) Sharing a friend's post

    (b) Tagging a friend in a photo

    (c) Sharing personal contact information

    (d) Posting a status update

4. Which of the following is an effect of revelation in OSM? (CO2, K1)

   (a) Identity theft

   (b) Cyberstalking

   (c) Online harassment

   (d) All of the above

5. What is the primary goal of tracking social footprint in social media forensics? (CO3, K1)

   (a) To monitor social media activity

   (b) To identify online threats

   (c) To gather evidence for investigations

   (d) To understand online behavior

6. Which of the following is a characteristic of fraudulent entities in online social networks? (CO3, K1)

   (a) Consistent profile information

   (b) Inconsistent profile information

   (c) High engagement rates

   (d) Low engagement rates

7. What is the primary goal of spam detection in social media forensics? (CO4, K1)

   (a) To identify malicious content

   (b) To remove unwanted content

   (c) To prevent fake accounts

   (d) To detect phishing attacks

8. What is the primary goal of data collection in social media forensics? (CO4, K1)

   (a) To gather evidence for investigations

   (b) To understand online behavior

   (c) To identify online threats

   (d) To monitor social media activity

9. What is the purpose of sentiment analysis in social media data analysis? (CO5, K1)

   (a) To identify positive and negative opinions

   (b) To track engagement metrics

   (c) To monitor brand mentions

   (d) To understand user behavior

10. Which of the following open-source tools is used for social media monitoring? (CO5, K1)

   (a) TweetDeck

   (b) Hootsuite

   (c) Opensource Social Media Monitoring Tool (OSM)

   (d) All of the above

Part B (5 × 5 = 25)

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

11. (a) What is online social network? Explain it (CO1, K4)

Or

   (b) Discuss about cybercrime awareness (CO1, K4)

12. (a) Discuss the information privacy disclosure(CO2, K4)

Or

   (b) What is OSM? Explain it. (CO2, K2)

13. (a) Explain about taking social foot print. (CO3, K5)

Or

   (b) Discuss about policing and OSM (CO3, K4)

14. (a) Discuss the detection of spam. (CO4, K4)

Or

   (b) Discuss about the content on social media (CO4, K4)

15. (a) Discuss about open–source tools (CO5, K4)

Or

(b) Explain the IT rules 2021 (CO5, K5)

Part C (5 × 8 = 40)

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

16. (a) Discuss the challenges in social media (CO1, K4)

Or

(b) Explain the scrapping data from social media APIs (CO1, K5)

17. (a) Illustrate the revelation and its effects in OSM (CO2, K4)

Or

(b) Explain privacy issues in social media (CO2, K5)

18. (a) Explain identifying fraudulent entities in online social network. (CO3, K5)

Or

(b) Discuss in detail about privacy setting policies on OSM (CO3, K4)

19. (a) Explain about: (CO4, K5)

(i) Phishing,

(ii) frauds

Or

(b) Discuss about data collection and analysis (CO4, K4)

20. (a) Discuss about safety on social media (CO5, K4)

Or

(b) Discuss about legal issues in social media (CO5, K4)

R2095

Sub. Code
556507

M.Sc. DEGREE EXAMINATION, NOVEMBER – 2024

Third Semester

Cyber Forensics

Elective : DATA ANALYTICS AND PRIVACY

(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 characteristic of big data veracity? (CO1, K1)

   (a) Accurate data (b) Inaccurate data

   (c) Reliable data (d) Unreliable data

2. Which type of analytics helps in identifying the cause of a problem? (CO1, K1)

   (a) Descriptive Analytics

   (b) Predictive Analytics

   (c) Prescriptive Analytics

   (d) Diagnostic Analytics

3. Who is responsible for defining the business requirements for a data analytics project? (CO2, K1)

   (a) Data analyst (b) Business stakeholder

   (c) IT Support (d) Data Scientist

4. What is the purpose of data normalization? (CO2, K1)

(a) To scale numeric values

(b) To encode categorical variables

(c) To remove duplicates

(d) To handle missing values

5. What is clustering in data analytics? (CO3, K1)

(a) A supervised learning technique

(b) An unsupervised learning technique

(c) A reinforcement learning technique

(d) A deep learning technique

6. What is the purpose of the confidence measure in the Apriori algorithm? (CO3, K1)

(a) To evaluate the support of a rule

(b) To evaluate the lift of a rule

(c) To determine the strength of a rule

(d) To determine the correlation between items

7. What is HDFS? (CO4, K1)

(a) A distributed database management system

(b) A distributed file system

(c) A data processing engine

(d) A data analytics tool

8. What is data warehousing in database analytics? (CO4, K1)

(a) A process of storing data in a database

(b) A process of analyzing data in a database

(c) A process of retrieving data from a database

(d) A process of integrating data from multiple sources

9. Which of the following is a key principle of data privacy? (CO5, K1)

(a) Data minimization

(b) Data maximization

(c) Data sharing

(d) Data storage

10. What is data anonymization? (CO5, K1)

(a) Removing personal identifiers from data

(b) Encrypting data

(c) Hashing data

(d) All of the above

Part B (5 × 5 = 25)

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

11. (a) What is Classification of digital data? Explain it. (CO1, K4)

Or

(b) Discuss top analytic tools. (CO1, K4)

12. (a) Discuss about framing the problem. (CO2, K4)

Or

(b) Illustrate Model selection. (CO2, K3)

13. (a) Explain about K–Means clustering algorithm. (CO3, K4)

Or

(b) Explain the representing text. (CO3, K5)

14. (a) Discuss about use case model in data analytics. (CO4, K4)

Or

(b) Discuss about MADlib. (CO4, K4)

15. (a) Discuss about ethical considerations in data analytics. (CO5, K4)

Or

(b) Explain personalize in data privacy. (CO5, K5)

Part C (5 × 8 = 40)

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

16. (a) Briefly explain about challenges with big data. (CO1, K5)

Or

(b) Explain the terminologies used in big data environments. (CO1, K5)

17. (a) Explain the learning business domain. (CO2, K5)

Or

(b) Discuss about operationalize. (CO2, K4)

18. (a) Explain the Association rules. (CO3, K5)

Or

(b) Discuss in detail about Decision tree. (CO3, K4)

19. (a) Elaborately discuss about Apache Hadoop.(CO4, K4)

Or

(b) Discuss about user define functions and aggregations. (CO4, K4)

20. (a) Discuss about data privacy laws and regulations. (CO5, K4)

Or

(b) Discuss about the balancing or counter intelligence. (CO5, K4)

———————