D–8034	Sub. Code
	51911

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
MAY 2025.

First Semester

CRYPTOGRAPHY AND NETWORK SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — ($10 \times 2 = 20$ marks)

Answer ALL the questions.

1. What is the primary purpose of a security mechanism?

2. What is meant by 'plaintext' and 'ciphertext' in encryption?

3. What is the basic principle behind block ciphers?

4. What is finite field arithmetic, and how is it used in AES?

5. Name the main components of the EIGamal cryptographic system.

6. Define pseudorandom number generation.

7. Define a message authentication code.

8. Write a short note on digital signatures.

9. What is the primary goal of web security?

10. Define IP security policy.

PART B — ($5 \times 5 = 25$ marks)

Answer ALL questions, choosing either (a) or (b).

11. (a) Explain the significance of the OSI security architecture in modern network security.

Or

(b) Describe the different types of security attacks and provide an example for each.

12. (a) Explain the concept of linear cryptanalysis and its impact on DES security.

Or

(b) Discuss the challenges associated with implementing AES in hardware and software.

13. (a) Analyze the principles of public-key cryptosystems.

Or

(b) Describe the process of key exchange in the Diffie-Hellman protocol.

14. (a) Discuss the advantages and limitations of using MAC-based ciphers for message authentication.

Or

(b) Discuss the Digital Signature Standard (DSS), its components, and its importance in digital authentication.

15. (a) Describe the role of the secure sockets layer (SSL) in securing web communication.

Or

(b) Discuss the potential vulnerabilities in web security and how they can be mitigated.

PART C — ($3 \times 10 = 30$ marks)

Answer any THREE questions.

16. Analyze the advantages and disadvantages of symmetric cipher models compared to asymmetric cipher models.

17. Describe the key expansion process in AES and its importance for encryption security.

18. Discuss the workings of the RSA algorithm in detail.

19. Analyze the Schnorr digital signature scheme and compare its efficiency and security with other digital signature methods.

20. Describe the process of email encryption using Pretty Good Privacy.

———————

D–8035	Sub. Code
	51912

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
MAY 2025.

First Semester

FUNDAMENTALS OF CYBER SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — ($10 \times 2 = 20$ marks)

Answer ALL the questions.

1. What are the different classifications of cyber criminals?

2. Define cryptocurrency and give an example.

3. What is wireless forensics?

4. How does malware forensics differ from other types of forensics?

5. Explain the term “network hacking”.

6. What is meant by malware in the context of ethical hacking?

7. Why is training and education important in handling digital evidence?

8. What are the obstacles faced during evidence collection?

9. Define system integrity validation.

10. What is unauthorized access by an outsider?

PART B — ($5 \times 5 = 25$ marks)

Answer ALL questions, choosing either (a) or (b).

11. (a) Discuss the role and importance of database forensics in investigating cybercrimes.

Or

(b) Explain the techniques involved in mobile forensics.

12. (a) How is web hacking performed? Discuss its implications.

Or

(b) Explain the different types of cracking methods used in ethical hacking.

13. (a) Discuss the significance of volatile evidence in digital forensics.

Or

(b) What are the types of evidence that can be collected in a digital investigation?

14. (a) Explain network-based intrusion detection systems (NIDS) and how they function.

Or

(b) Discuss the concept of security information management and its relevance in modern cybersecurity.

15. (a) Describe the vulnerabilities associated with complex network architectures.

Or

(b) What is the role of biometrics in enhancing cybersecurity?

PART C — ($3 \times 10 = 30$ marks)

Answer any THREE questions.

16. Discuss the challenges and methodologies involved in conducting wireless forensics and database forensics.

17. Explain the process of hacking windows systems and discuss the countermeasures to protect against such attacks.

18. Analyze the obstacles and solutions in evidence collection during digital investigations.

19. Discuss the importance of network session analysis and its impact on identifying and preventing cyber threats.

20. Evaluate the vulnerabilities in software systems and propose measures to enhance cyber security.

———————

D–8036

Sub. Code
51913

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
MAY 2025.

First Semester

CYBER SECURITY LAW AND PRACTICE

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — ($10 \times 2 = 20$ marks)

Answer ALL the questions.

1. Why was the IT Act, 2000 enacted in India?

2. What are the powers of authorities under the IT Act, 2000?

3. How does the IT Act influence the Bankers Book Evidence Act?

4. What does cyber space jurisdiction entail?

5. Define E-Governance and its significance in Indian law.

6. What are the challenges in E-Taxation within cyberspace?

7. What are the implications of cyber squatting on trademark disputes?

8. Explain the role of copyright in computer programs.

9. Name two types of cyber crimes against the nation.

10. Mention a significant case law related to cyber crime in India.

PART B — ($5 \times 5 = 25$ marks)

Answer ALL questions, choosing either (a) or (b).

11. (a) Explain the amendments made to the India Penal Code concerning cyber law.

Or

(b) Discuss the concept of cyber space jurisdiction and its importance.

12. (a) How does the Indian law regulate digital signatures?

Or

(b) Analyze the provisions of E-commerce under Indian Law.

13. (a) Discuss the impact of cyber squatting on intellectual property rights.

Or

(b) Explain the challenges of copyright protection in the digital medium.

14. (a) Describe the legal measures in India to combat cyber crimes against property.

Or

(b) Discuss how Indian law addresses cyber crimes against individuals.

15. (a) Outline the key features of cyber laws in the United Kingdom.

Or

(b) Explain the Australian laws related to privacy in the context of cyber security.

PART C — ($3 \times 10 = 30$ marks)

Answer any THREE questions.

16. Discuss in detail the amendments made to the Reserve Bank of India Act concerning cyber law.

17. Evaluate the legal validity of E-Contracts in India and the challenges associated with them.

18. Analyze the role of intellectual property rights in the Internet era, with a focus on domain names and trademarks.

19. Critically assess the legal framework in India for addressing cyber crimes against property and individuals.

20. Compare the cyber laws of Malaysia and the Netherlands, highlighting their approaches to privacy and cybercrime.

———————

D–8037	Sub. Code
	51921

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
MAY 2025.

Second Semester

WEB APPLICATION SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — ($10 \times 2 = 20$ marks)

Answer ALL the questions.

1. Define HTTP.

2. What does IIS stand for?

3. Mention any two types of web penetration testing.

4. Comment on SQL injection.

5. Define client-side controls in web applications.

6. What is the purpose of bypassing client-side controls in penetration testing?

7. How does a brute force attack work?

8. What is credential stuffing?

9. Mention two common types of XSS attacks.

10. Define API security in web applications.

PART B — ($5 \times 5 = 25$ marks)

Answer ALL questions, choosing either (a) or (b).

11. (a) Compare client-side scripting and service-side scripting with examples.

Or

(b) Explain the role of IIS in Windows-based web hosting.

12. (a) Identify and explain the key phases of web penetration testing methodology.

Or

(b) What are the limitations of web penetration testing? Discuss in detail.

13. (a) Describe how attackers bypass client-side validation with an example.

Or

(b) How do security researchers identify and exploit vulnerabilities in modern web applications?

14. (a) What are the different types of authentication attacks in web applications? Classify and explain.

Or

(b) What do you mean by session fixation? How it can be prevented.

15. (a) Explain how attackers exploit weak authentication mechanisms.

Or

(b) Describe different methods of securing API endpoints.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Discuss different network topologies and their advantages and disadvantages.

17. Describe how SQL Injection attacks are detected and prevented in web penetration testing.

18. Categorize various techniques used to bypass client-side controls in web applications.

19. How do attackers exploit session management vulnerabilities? Discuss.

20. Summarize the various types of cross-site scripting attacks and their prevention techniques.

———————

D–8038	Sub. Code
	51922

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
MAY 2025.

Second Semester

MALWARE ANALYSIS AND NETWORK SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — ($10 \times 2 = 20$ marks)

Answer ALL the questions.

1. Define Antivirus scanning.

2. What is the role of virtual machines in malware analysis?

3. Write an example of a simple ADD instruction in assembly.

4. Identify the role of the CALL instruction in function calls.

5. What is the difference between kernel-mode and user-mode debugging?

6. What is the role of a malware sandbox?

7. How does a firewall enhance network security?

8. What is the purpose of syslog in network security?

9. What is the role of port stealing in LAN attacks?

10. What is the purpose of SCP?

PART B — ($5 \times 5 = 25$ marks)

Answer ALL questions, choosing either (a) or (b).

11. (a) Discuss the advantages of using virtual machines in malware analysis.

Or

(b) Differentiate between static and dynamic malware analysis with examples.

12. (a) Describe the importance of registers in the x86 architecture.

Or

(b) Explain how the C main ( ) method interacts with assembly, including offsets and calling conventions.

13. (a) Explain how system calls and API calls are used in malware behavior analysis.

Or

(b) Describe the process of patching malware and its significance.

14. (a) Explain how stateful firewalls improve upon traditional packet filtering firewalls.

Or

(b) Evaluate the importance of network log management in detecting cyber threats.

15. (a) Explain the step-by-step process of a Man-in-the-Middle attack.

Or

(b) What is SSL stripping? How do attackers use it to downgrade encryption?

PART C — ($3 \times 10 = 30$ marks)

Answer any THREE questions.

16. Discuss the importance of sandboxing and how it aids in malware behavior analysis.

17. How are arithmetic operations performed in x86 assembly? Provide examples.

18. Demonstrate the complete process of live malware analysis with tools and techniques.

19. How can Splunk be used to collect, analyze and visualize network security logs? Provide a step-by-step approach.

20. Describe the concept, working and impact of ARP poisoning in LAN attacks.

———————

D–8039

Sub. Code
51923

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
MAY 2025.

Second Semester

MOBILE SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — ($10 \times 2 = 20$ marks)

Answer ALL the questions.

1. What is Android?

2. Mention any two components of the Android Framework.

3. Name any two types of Android permissions.

4. Define content provider permission.

5. Comment on APK file.

6. Define package verification in Android.

7. What is the primary user in Android?

8. How does Android handle app installations for multiple users?

9. What is Public Key Infrastructure?

10. What is a screen lock, and how does it help in device security?

PART B — ($5 \times 5 = 25$ marks)

Answer ALL questions, choosing either (a) or (b).

11. (a) Explain the different versions of Android with at least three examples.

Or

(b) What are intents and how are they used in Android applications?

12. (a) Differentiate between system permissions and custom permissions.

Or

(b) Discuss granting and revoking permissions in Android.

13. (a) Describe the steps involved in the APK installation process.

Or

(b) Explain the role of the Android Package Manager in APK installation.

14. (a) Outline the concept of user management in Android.

Or

(b) Discuss the role of guest users and their limitations in Android.

15. (a) List the Android's network security features? Explain it in detail.

Or

(b) Explain the importance of encryption in Android security.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Demonstrate the Android Architecture in detail with a neat diagram.

17. Discuss the Android's permission model in detail.

18. Examine the APK file format in detail with a diagram.

19. Explain Android User Management in detail with different user types.

20. Describe the role of credential storage and how android secures sensitive information.

———————