D–1036	Sub. Code
	51911

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2025.

First Semester

CRYPTOGRAPHY AND NETWORK SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — (10 × 2 = 20 marks)

Answer ALL questions.

1. What is meant by entity authentication?

2. Define monoalphabetic substitution.

3. What is a block cipher?

4. State the main idea behind linear cryptanalysis.

5. List out the keys used in public key cryptography.

6. Define pseudorandom number generator (PRNG).

7. What are the requirements of message authentication?

8. Mention any two advantages of HMAC.

9. Digital Signature Standard (DSS).

10. What is the main goal of web security?

PART B — (5 × 5 = 25 marks)

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

11. (a) Explain the components of OSI security architecture.

Or

(b) Describe the process of encryption technique with an example.

12. (a) Describe the structure of the DES algorithm.

Or

(b) Elaborate the function of SubBytes and ShiftRows transformations in AES.

13. (a) Write down the steps involved in RSA key generation process.

Or

(b) Explain the Diffie-Hellman key exchange algorithm with an example.

14. (a) Briefly explain the security aspects of MACs.

Or

(b) Discuss how a MAC is generated and verified using HMAC.

15. (a) Estimate the role of Pretty Good Privacy (PGP) in email security.

Or

(b) Elaborate any five web security considerations.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Describe the various types of security attacks in detail.

17. Analyze the implementation of AES in hardware and software.

18. Evaluate the mechanism of RSA and ElGamal cryptosystems.

19. Discuss different techniques used for message authentication.

20. Elaborate the architecture of IP security.

———————

D–1037	Sub. Code
	51912

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2025.

First Semester

FUNDAMENTALS OF CYBER SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — (10 × 2 = 20 marks)

Answer ALL the questions.

1. What do you mean by Cyber Crime?

2. Define Malware.

3. What is Network Forensics?

4. Give two examples of database forensics tools.

5. What is a vulnerability?

6. Give an example of digital evidence.

7. Expand NIPS and HIPS.

8. What is an unauthorized access?

9. List any two benefits of using a Host-based intrusion prevention system.

10. Name two common cyber threats that exploit system vulnerabilities.

PART B — (5 × 5 = 25 marks)

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

11. (a) Discuss the tools used in cyber crime.

Or

(b) Explain the technology behind Bitcoin.

12. (a) Write and explain the steps involved in performing mobile forensics.

Or

(b) Differentiate threat and vulnerability with suitable examples.

13. (a) Why is volatile evidence critical in digital investigations? Give examples.

Or

(b) Explain the different types of malwares used in hacking.

14. (a) Describe how intrusions can be detected and mitigated.

Or

(b) Elaborate system integrity validation with examples.

15. (a) Discuss common vulnerabilities in software applications.

Or

(b) Describe the security risks associated with complex network architectures.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Explain how Blockchain works and discuss its applications.

17. Compare and contrast black hat, white hat, and grey hat hackers.

18. Discuss the importance of training and education in handling digital evidence.

19. Explain the risks and consequences of physical theft in information systems.

20. Describe weak authentication. What are the best practices for strengthening authentication mechanisms?

———————

D–1038

Sub. Code
51913

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2025.

First Semester

CYBER SECURITY LAW AND PRACTICE

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — (10 × 2 = 20 marks)

Answer ALL the questions.

1. Define cyber law.

2. State two salient features of the IT Act, 2000.

3. What is cyber space jurisdiction?

4. Name two Acts amended due to cyber law requirements.

5. Define E-commerce in simple terms.

6. What is a digital signature under Indian law?

7. What is cyber squatting?

8. State two examples of copyright in computer programs.

9. Define cybercrime against Individual.

10. Name any two Indian case laws on cybercrime.

PART B — (5 × 5 = 25 marks)

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

11. (a) Explain the evolution and need for the IT Act, 2000.

Or

(b) Discuss penalties and offences under the IT Act.

12. (a) Describe amendments to the Indian Penal Code related to cyber law.

Or

(b) Explain the impact of cyber law on the Bankers book evidence Act.

13. (a) Explain the concept of E-Governance and its practicality in India.

Or

(b) Write a short note on E-taxation issues in cyberspace.

14. (a) Discuss domain names and trademark disputes in cyberspace.

Or

(b) Explain reverse Hijacking with an example.

15. (a) Explain cyber crime against property with examples.

Or

(b) Discuss crime against nation in the cyber context.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Critically analyze the genesis and necessity of cyber law in India.

17. Explain cyber space jurisdiction in detail with examples and challenges.

18. Discuss E-commerce provisions in Indian law and the role of electronic contracts.

19. Explain intellectual property rights in cyberspace with focus on trademarks and copyright.

20. Describe Indian case laws related to cyber crime and their significance.

———————

D–1039	Sub. Code
	51921

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2025.

Second Semester

WEB APPLICATION SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — (10 × 2 = 20 marks)

Answer ALL the questions.

1. Define HTML.

2. Name two web servers used in Windows and Linux.

3. What is web penetration testing?

4. Define the term “black box testing” in penetration testing.

5. Comment on web application mapping.

6. Identify two common techniques used to bypass client-side validation.

7. Define session hijacking.

8. How does an attacker exploit weak password policies?

9. Define command injection in web security.

10. What is the purpose of authentication in web security?

PART B — (5 × 5 = 25 marks)

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

11. (a) Outline the basic structure of an HTML document with an example.

Or

(b) Explain the concept of DMZ in networking.

12. (a) Classify the different types of web penetration testing.

Or

(b) Discuss how cross-site scripting attacks are identified in penetration testing.

13. (a) Compare different web application technologies and their security implications.

Or

(b) Describe the impact of server-side request forgery in web applications.

14. (a) Examine the concept of password attacks with examples.

Or

(b) Describe broken authentication and its risks.

15. (a) Discuss how automated attack tools are used in penetration testing.

Or

(b) How do attackers exploit vulnerabilities in application servers?

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Explain the web server architecture and how it handles client requests.

17. Demonstrate the complete web penetration testing methodology with steps and examples.

18. Discuss the complete process of mapping a web application and identifying security weaknesses.

19. Categorize the different types of access control attacks and their impact on web applications.

20. Examine the different techniques used to attack back-end components in web applications.

———————

D–1040	Sub. Code
	51922

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2025.

Second Semester

MALWARE ANALYSIS AND NETWORK SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — (10 × 2 = 20 marks)

Answer ALL the questions.

1. What is malware analysis?

2. Define sandboxing in malware analysis.

3. What is the role of main memory in the x86 architecture?

4. Identify the purpose of the .text and .data sections in a PE file.

5. What is the difference between live and dead malware analysis?

6. Mention two common anti-dynamic analysis techniques.

7. What is the function of an application-aware firewall?

8. Differentiate between honeypots and honeynets.

9. How do Man-in-the-Middle attacks work?

10. Define IPSec and its role in secure network communication.

PART B — (5 × 5 = 25 marks)

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

11. (a) Explain the importance of hashing in malware detection.

Or

(b) Describe the basic steps involved in dynamic malware analysis.

12. (a) Classify the different types of x86 instructions with examples.

Or

(b) Examine the importance of function analysis in IDA Pro.

13. (a) Discuss common evasion techniques used by malware to bypass detection.

Or

(b) Differentiate between kernel-mode debugging and user-mode debugging.

14. (a) Analyze the role of proxies in content filtering and network security.

Or

(b) Implement and analyze NAT and firewall rules to prevent unauthorized access in a multi-layered network.

15. (a) Describe how an attacker can use port stealing to hijack a session.

Or

(b) How does single sing-on enhance authentication security?

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Discuss various static analysis tools and their roles in malware investigation.

17. Explain in detail the structure of the PE file and its major sections.

18. Explain in detail how a malware sandbox works and its role in analysis.

19. Analyze the compare different firewall types with examples.

20. Demonstrate and analyze the working of SSH and SCP in a secure communication setup.

———————

D–1041	Sub. Code
	51923

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2025.

Second Semester

MOBILE SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — (10 × 2 = 20 marks)

Answer ALL questions.

1. Define Android architecture.

2. What is the role of the Linux Kernel in Android?

3. What is permission in Android?

4. How does Android inform users about app permissions?

5. Mention any two essential components of an APK file.

6. What is the first step in the APK installation process?

7. Define guest user in Android.

8. What is external storage in Android?

9. What is credential storage in Android?

10. Define enterprise security in Android.

PART B — (5 × 5 = 25 marks)

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

11. (a) Describe the four layers of Android architecture.

Or

(b) How does Android ensure security for applications?

12. (a) What is the role of content provider permissions? Give an example.

Or

(b) Describe the different protection levels of permissions in Android.

13. (a) Explain the structure of an APK file with its key components.

Or

(b) What are the different ways to install an APK on an Android device? Discuss.

14. (a) Classify the different types of users in Android.

Or

(b) What are the security risks of external storage in Android? Discuss.

15. (a) Examine the Public Key Infrastructure and its components.

Or

(b) Categorise the different types of credential storage mechanisms in Android.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Demonstrate the components of the android framework and their importance.

17. Discuss the different types of android permissions and their use cases.

18. Illustrate the importance of code signing and how it prevents security threats.

19. Explain the role of user metadata and how android maintains user data.

20. What are the different authentication methods available for securing Android devices? Discuss.

———————