D–2035	Sub. Code
	51911

DISTANCE EDUCATION

DIPLOMA IN (Cyber Security) EXAMINATION, MAY 2026.

First Semester

CRYPTOGRAPHY AND NETWORK SECURITY

(CBCS 2021 Calender Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — (10 × 2 = 20 marks)

Answer ALL the questions.

1. Define security attack.

2. What is the purpose of digital signatures?

3. What is known as brute-force attack?

4. Mention two challenges in implementing AES.

5. State the key generation steps in RSA.

6. Write the two phases of ElGamal encryption process.

7. What do you mean by Message Authentication Code (MAC)?

8. Define block cipher.

9. Write the definition of ElGamal digital signature scheme.

10. What is TLS used for?

PART B – (5 × 5 = 25 marks)

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

11. (a) Discuss about security mechanisms in the OSI Security Architecture.

Or

(b) Explain the importance of authentication and confidentiality.

12. (a) Describe the vulnerabilities of DES.

Or

(b) Elaborate the principles of designing a secure block cipher.

13. (a) Explain the concept of elliptic curve cryptography.

Or

(b) Analyze the strengths and weaknesses of Diffie - Hellman key exchange method.

14. (a) Describe the working principles of CMAC.

Or

(b) Discuss the MACs based on hash functions.

15. (a) Explain the Schnorr Digital Signature Scheme.

Or

(b) Give an overview of IP Security (IPsec) and its main components.

PART C – (3 × 10 = 30 marks)

Answer any THREE questions

16. Describe the network security model with a neat diagram.

17. Evaluate the mechanism of differential and linear cryptanalysis.

18. Explain the principles of public key cryptosystems.

19. Discuss in detail about security benefits of HMAC.

20. Determine the functions of Encapsulating Security Payload (ESP) in IPsec.

———————

D–2036

Sub. Code
51912

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
MAY 2026.

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 questions.

1. Who are the Professional Hackers?

2. What is a Bitcoin?

3. Mention any two tasks involved in Disk Forensics.

4. What is Email Forensics?

5. Define SQL injection.

6. What is the role of education in digital forensics?

7. Define volatile evidence.

8. State the role of anti-malware software.

9. What is meant by data seizure?

10. Give two examples of software vulnerabilities.

PART B – (5 × 5 = 25 marks)

Answer ALL Questions

11. (a) Describe the concept of Cryptocurrency.

Or

(b) Explain in detail about blockchain technology.

12. (a) Discuss the challenges faced in Wireless Forensics.

Or

(b) Describe any three methods used to crack passwords.

13. (a) List and briefly explain different types of digital evidence.

Or

(b) Discuss the common objectives of an ethical hacker during a penetration test.

14. (a) Explain the methodology of unauthorized access by outsiders.

Or

(b) Elaborate the concept of Security Information Management (SIM).

15. (a) Explain how poor system administration can lead to security vulnerabilities.

Or

(b) What is biometrics in Cyber security? Explain their advantages and limitations.

PART C – (3 × 10 = 30 marks)

Answer any THREE Questions

16. Describe the categories and motives of Cyber Criminals.

17. Describe common techniques used to exploit vulnerabilities in Windows operating systems.

18. Analyze the standard procedures followed during a digital forensic investigation.

19. Analyze Host-based Intrusion Prevention Systems (HIPS).

20. Explain different authentication methods with their advantages and limitations.

———————

D–2037	Sub. Code
	51913

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
MAY 2026.

First Semester

CYBER SECURITY LAW & PRACTICE

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — (10 × 2 = 20 marks)

Answer ALL the questions.

1. What is the objective of the IT Act, 2000?

2. Name any two authorities under the IT Act.

3. Define the Indian Penal Code amendment in cyber context.

4. What is the Reserve Bank of India's role in cyber laws?

5. State two e-commerce issues in Indian law.

6. What is an e-contract?

7. Define Reverse Hijacking.

8. Mention two key aspects of trademark disputes online.

9. What is cybercrime against Property?

10. Name two types of crime against Nation.

PART B — (5 × 5 = 25 marks)

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

11. (a) Discuss the salient features of the IT Act, 2000.

Or

(b) Explain the various authorities and their powers under the IT Act.

12. (a) Explain cyber space jurisdiction challenges.

Or

(b) Describe the amendments to the Indian Evidence Act.

13. (a) Discuss legality and validity of e-contracts in India.

Or

(b) Write a note on the Cyber Tribunal and Appellate Tribunal.

14. (a) Explain copyright in the digital medium with examples.

Or

(b) Discuss the concept of cyber-squatting with case examples.

15. (a) Describe crimes against Individual with examples.

Or

(b) Discuss Indian case laws on cyber crime.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Explain in detail the evolution of the IT Act, 2000 and its salient features.

17. Analyze amendments to Indian Penal Code, Evidence Act, and RBI Act due to cyber law.

18. Explain E-Governance in India, its concept, challenges, and benefits.

19. Discuss Intellectual Property Rights in cyberspace with focus on cyber squatting and domain disputes.

20. Compare International Cyber Laws: US and UK perspectives.

———————

D–2038

Sub. Code
51921

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
MAY 2026.

Second Semester

WEB APPLICATION SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — (10 × 2 = 20 marks)

Answer ALL questions.

1. What is HTTP?

2. Define Client-side scripting with example.

3. What is Web Penetration Testing?

4. Name two types of Web Penetration Testing.

5. What is Application Mapping?

6. Define Client-side Controls.

7. What is Session Management?

8. Define Access Control.

9. What is Cross-Site Scripting (XSS)?

10. Name two attacks targeting Users other than XSS.

PART B — (5 × 5 = 25 marks)

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

11. (a) Explain HTTP 1.0 and HTTP 1.1 differences.

Or

(b) Describe Web Server Architecture for Windows and Linux.

12. (a) Describe the Web Penetration Testing Methodology.

Or

(b) Explain Core Defense Mechanisms in Web Security.

13. (a) Explain Bypassing Client-side Controls with examples.

Or

(b) Discuss Mapping a Web Application for security testing.

14. (a) Discuss attacks on Session Management with techniques.

Or

(b) Explain attacks on Authentication systems.

15. (a) Explain Cross-Site Scripting with types and examples.

Or

(b) Describe attacks on Back-End Components.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Discuss Web Fundamentals including HTML, Client-side and Server-side scripting with examples.

17. Explain in detail the Web Penetration Testing Approach and its steps.

18. Describe Web Application Technologies, Application Mapping and Bypassing Client-side Controls.

19. Analyze attacks on Authentication, Session Management and Access Controls.

20. Explain attacks targeting Users (XSS and other techniques) and attacks on Back-End Components.

———————

D–2039	Sub. Code
	51922

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
MAY 2026.

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. Write the primary goal of malware analysis.

2. What is the role of AV scanning in malware analysis?

3. Mention the importance of registers in x86 architecture?

4. What is Global variable?

5. Define live malware analysis.

6. List any two anti-dynamic analysis tricks used by modern malware.

7. Write the key difference between a packet-filter firewall and a stateful firewall.

8. Define a honeypot.

9. Describe ARP cache poisoning.

10. Which OSI layer does VLAN hopping exploit?

PART B — (5 × 5 = 25 marks)

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

11. (a) What are the key components of the PE (Portable Executable) file format?

Or

(b) Mention the importance of virtual machines in malware analysis.

12. (a) Discuss the useful Windows for analysis.

Or

(b) Describe conditional branching with an example.

13. (a) Explain the procedure to capture and analyse a sample's network activity with Wireshark.

Or

(b) Kernel-mode vs User-mode debugging — contrast them.

14. (a) How a personal firewall using iptables secures a Linux system?

Or

(b) How does a proxy server protect a network?

15. (a) Describe how a Man-in-the-Middle (MITM) attack using ARP spoofing works on a switched LAN.

Or

(b) Outline the workflow for cracking a Linux shadow file.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Elucidate the Static Analysis and Dynamic Analysis.

17. Describe how IDA Pro aids in function analysis and graphing.

18. Develop an end-to-end workflow for analysing an unknown Windows malware sample.

19. Explain the working of Snort as an Intrusion Detection System.

20. Give a Lab Demonstration of VLAN Hopping.

———————

D–2040	Sub. Code
	51923

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
MAY 2026.

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. What is the role of mobile security?

2. Mention the architectural layers.

3. Differentiate normal and dangerous permissions in Android.

4. Why are the content provider permissions necessary?

5. What is an APK file in Android?

6. Write a note on the META-INF/ directory in an APK.

7. Give a note on user management in Android.

8. How is the external storage isolated between users in Android?

9. Discuss the role of the Java Cryptography Architecture (JCA).

10. Define Cryptographic Service Provider (CSP) in Java.

PART B — (5 × 5 = 25 marks)

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

11. (a) Explain the components of the Android Architecture.

Or

(b) Describe the layers of Android Architecture and their role in security.

12. (a) How does permission enforcement work in the Android security model?

Or

(b) Explain the URI-based permissions work with content providers.

13. (a) Discuss the role of code signing in Android APK security.

Or

(b) What are the steps involved in verifying an APK during installation?

14. (a) Describe the different types of users supported by Android.

Or

(b) How does Android handle per-user app installation and management?

15. (a) List out JCA Engine Classes with their purpose.

Or

(b) Explain the purpose of credential storage and how Android manages it securely.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Describe the Android Security Model and the Android Framework.

17. Discuss the types of permissions in Android, including system and custom permissions.

18. Explain the steps involved in its installation and package verification process.

19. How does android manages users and their metadata?

20. Write a detail note on Android that provides security through cryptographic service provider.

———————