D–1040	Sub. Code
	51911

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2021.

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 questions.

1. Differentiate passive attack from active attack with example.

2. What are the two basic functions used in encryption algorithms?

3. Define Block Cipher.

4. Mention the Substitute byte transformation in AES.

5. Write about elliptic curve cryptography.

6. Specify the applications of public key cryptosystem.

7. What is the role of compression function in hash function?

8. List out the attacks on MAC.

9. Define key Identifier.

10. What are the properties of digital signature should have?

PART B — ($5 \times 5 = 25$ marks)

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

11. (a) Explain the components of encryption algorithm.

Or

(b) Discuss in detail (i) Security Services (ii) Security Mechanism.

12. (a) Illustrate AES Structure in detail.

Or

(b) Explain the differential and Linear Cryptanalysis.

13. (a) What requirements must a public key cryptosystem to fulfill to a secured algorithm? Explain.

Or

(b) Explain USA algorithm.

14. (a) How the security of MAC expressed? Explain.

Or

(b) What is the role of compression function in hash function? Discuss.

15. (a) Write a detailed note on Digital signatures.

Or

(b) Distinguish between direct and arbitrated digital signature.

PART C — ($3 \times 10 = 30$ marks)

Answer any THREE questions.

16. Explain about OSI Security architecture model with neat diagram.

17. Discuss in detail about DES.

18. Describe the decryption process in EIGamal cryptosystem.

19. Explain Message Authentication codes and its functions.

20. Write detail about

    (a) Pretty Good Privacy

    (b) IP security Overview

    (c) IP Security Policy

    (d) Encapsulating Security Payload.

———————

D–1041

Sub. Code
51912

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2021.

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. What distinguishes cybercrime from traditional criminal activity?

2. Define the term Hacking' and explain its essentials.

3. What is Ransomware attack?

4. State the purpose of alert messages.

5. Write short notes of Hacking.

6. Define Brute Force Hack.

7. What is Onion Routing?

8. Explain Web shells.

9. List out the anti malware softwares.

10. What do you mean by web hacking?

PART B — ($5 \times 5 = 25$ marks)

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

11. (a) Explain the types of Cyber Crime.

Or

(b) What are the tools used in Cyber Crime? Explain.

12. (a) Write short notes on:

(i) Computer forensics services

(ii) Software forensics. Give example for each.

Or

(b) Explain MAC Spoofing in Wireless Networks.

13. (a) Write about (i) Ethical hacking in motion (ii) Hacking Network hosts.

Or

(b) Illustrate about foundation for ethical hacking.

14. (a) What are the steps to create image files of digital evidence? Explain.

Or

(b) What is Messenger forensic? State the different types of evidence that can be collected from a messenger? Where can such files be found on computer?

15. (a) Why should we use Anti-Malware Software? Explain.

Or

(b) Discuss about Intrusion detection and Prevention Techniques.

PART C — ($3 \times 10 = 30$ marks)

Answer any THREE questions.

16. What do you understand by the term 'Cyber Security'? Explain in brief the major security threats and Solutions.

17. Explain in detail about cyber security vulnerabilities.

18. Discuss in detail about Password hacking and Malware.

19. Enlighten the procedures for Corporate High-tech Investigations with respect to:

    (a) Employee Termination Cases

    (b) Internet Abuse Investigation

    (c) Email Abuse Investigation

    (d) Media Leak investigation.

20. Illustrate the overview of Cyber Security, Authentication, and Biometrics.

———————

D–1042	Sub. Code
	51913

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2021.

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 questions.

1. Define Cyber Law.

2. What is IT Act 2000?

3. What is an Amendment?

4. Define the term Hacking.

5. What is cyber space jurisdiction?

6. What do you mean by Digital signature?

7. Define Intellectual Property Right.

8. Define Cyber Squatting.

9. List out any two Cyber laws in India.

10. Give any two examples for Cyber Crime.

PART B — ($5 \times 5 = 25$ marks)

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

11. (a) Summarize the Evolution of IT Act.

Or

(b) Write short notes on the salient features of the IT Act, 2000.

12. (a) Give an overview of Indian Evidence Act.

Or

(b) Explain about Bankers Book Evidence Act.

13. (a) Write about the E-commerce Issues and Provisions in Indian Law.

Or

(b) Explain about the Taxation issues in Cyberspace.

14. (a) Briefly Explain about the concept of Trademarks in Internet Era.

Or

(b) Explain about Reverse Hijacking.

15. (a) Write short notes on Crime against Individual.

Or

(b) Briefly Explain about Crime against Property.

PART C — ($3 \times 10 = 30$ marks)

Answer any THREE questions.

16. Discuss about Penalties and Offences in Cyber Law.

17. Discuss in detail about Reserve Bank of Indian Act.

18. Explain about the E-Contracts and its validity in India.

19. Discuss about Copyright in Digital Medium.

20. Analyze in detail about the Indian Case Laws.

———————

D–1043

Sub. Code
51921

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY COURSE EXAMINATION, DECEMBER 2021.

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 questions.

1. Expand HTTP.
2. List out any two Network Topologies.
3. Mention the types of penetration testing.
4. How is Web Pen testing is done?
5. Mention any two Web Application Technologies.
6. What is client-side application security?
7. What is meant by Session Management?
8. How to attack access Controls?
9. List out Back End components.
10. What is an application attacks?

PART B — (5 × 5 = 25 marks)

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

11. (a) Write short note on: Network topologies.

Or

(b) Write short note on: IIS.

12. (a) Briefly Explain Web Penetration testing process.

Or

(b) Write short note on: Core Defense mechanisms.

13. (a) How to Bypassing the Client - Side Controls?

Or

(b) List out any two Web Application Technologies and explain them.

14. (a) Describe about the types of authentication in web applications security.

Or

(b) Explain the primary types of access Control.

15. (a) Explain about attacking Back-End Components.

Or

(b) What is web application attack and how to Defend against it?

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Discuss Web Server Architecture with neat diagram.

17. Describe Web Pen Testing methodology in detail.

18. Discuss about Client - Side Controls.

19. Describe the different attack on Session Management.

20. Explain About automating customized attack?

———————

D–1044	Sub. Code
	51922

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2021.

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 questions.

1. How does a packed malware work?

2. Why do we need static malware analysis?

3. What is PE in malware analysis?

4. What do mean by Graphing in malware analysis?

5. What is WORM?

6. What is a tracing?

7. What is Snort?

8. State the usage of SPLUNK.

9. Expand PGP, SSL.

10. What is Port Stealing?

PART B — ($5 \times 5 = 25$ marks)

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

11. (a) What is Virtual Machine? State its usage in Malware Analysis?

Or

(b) Give a note on salient features of Sandboxing.

12. (a) Give an overview of X86 Architecture.

Or

(b) Explain about Arithmetic Instructions in X86 Architecture.

13. (a) Write about the Malware Evasion Techniques.

Or

(b) Give a brief account on Exception Handling.

14. (a) What is Firewall? Explain about the types of Firewalls.

Or

(b) Briefly Explain about Signature based Anomaly Detection.

15. (a) Write short notes on DHCP Attacks.

Or

(b) Briefly Explain two main approaches of an intrusion detection techniques.

PART C — ($3 \times 10 = 30$ marks)

Answer any THREE questions.

16. Discuss about common Malware types, detection and removal mechanisms?

17. Discuss in detail about Portable Executable File Format?

18. Enumerate about the VM Detection techniques?

19. Discuss about Honeypots and Honeynets?

20. Briefly Discuss about the Dark Web and why it is illegal?

———————

D–1045	Sub. Code
	51923

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2021.

Second Semester

MOBILE SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

PART A — ($10 \times 2 = 20$ marks)

Answer ALL questions.

1. What are the code names of Android?

2. List out the Android Components.

3. Define Content Provider Permission.

4. Expand APK.

5. How does code signing protect a mobile app?

6. Define Metadata in mobile phone.

7. Expand JCA.

8. How to you provide Network Security?

9. What is meant by Credential storage?

10. Expand PKI.

PART B — ($5 \times 5 = 25$ marks)

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

11. (a) Write short note on: Android Frame work.

Or

(b) Write short note on functions of Android phone.

12. (a) Briefly Explain Permission Enforcement.

Or

(b) Write short note on: Custom Permission.

13. (a) Briefly Explain Code signing.

Or

(b) What is the use of APK Installer? Explain.

14. (a) Describe about User Metadata.

Or

(b) Explain about User Application Management.

15. (a) Explain about mobile network security.

Or

(b) Write short note on: Credential Storage.

PART C — ($3 \times 10 = 30$ marks)

Answer any THREE questions.

16. Discuss Android Architecture with Block Diagram.

17. Describe about System Permission.

18. How Package Verification is done in Android? Explain.

19. Explain in detail about different types of Mobile Device Security.

20. Discuss about Cryptographic Service Providers.

———————