D–7043

Sub. Code
51911

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2022.

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. 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 × 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 RSA 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 × 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 ElGamal 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–7044

Sub. Code

51912

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2022.

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 × 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 × 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–7045

Sub. Code
51913

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2022.

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 × 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 × 10 = 30 marks)

Answer any THREE questions.

16. Discuss about Penalties & Offences in Cyber Law.

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

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

19. Discuss about Copyright in Digital Medium.

20. Analyze in detail about the Indian Case Laws.

D–7046

Sub. Code
51921

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2022.

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 the role of Server?

2. Define HTML.

3. What do mean by search engine?

4. Write short notes about the client/server strategies in Internet.

5. Define Internet servers.

6. Define WWW.

7. What is the use of HTTP Protocol?

8. Define URL.

9. Write the format of HTML program.

10. Define Protocol.

PART B — (5 × 5 = 25 marks)

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

11. (a) Explain the purpose of Online Transactions? List out five websites that allow Online Transactions.

Or

(b) Explain secure Email protocols in detail.

12. (a) What are the major stages of risk assessment? Explain

Or

(b) Discuss the components of risk identification in detail.

13. (a) Write short notes on the access control devices used in security design

Or

(b) What is secure electronic transaction and how it can be achieved?

14. (a) Discuss about the issues in web security? Explain.

Or

(b) How does a client request a Transaction Server? Discuss

15. (a) List and Explicate the major protocols used for secure communications

Or

(b) Explain the role of Proxy server in web Security in detail.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Explain the Security architecture design process with a neat sketch Diagram.

17. How can you relate authentication functionality with application design?

18. Explain in detail about Firewall processing modes and its architecture.

19. Explain the roles of the different server in Kerberos protocol. How does the user get authenticated to the different servers?

20. What are the three types of security policies? Explain

D–7047

Sub. Code
51922

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2022.

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 questions.

1. What is non-Repudiation?

2. Define Two-Factor Authentication.

3. What is Command injection?

4. Distinguish between cyber war and cyber terrorism.

5. What is mutual authentication?

6. Which versions of IP can use IPsec?

7. What are reusable passwords?

8. Distinguish between IDS and IPS.

9. Define incident response in terms of planning.

10. Write a short note about command injection.

PART B — (5 × 5 = 25 marks)

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

11. (a) Design an Authentication System using Biometric Deception.

Or

(b) Explain the methods for enhancing Browser security.

12. (a) Discuss Principles of Business Continuity Management.

Or

(b) Explain about methods available for Network Intrusion Detection System.

13. (a) What is a DoS attack? Describe a DDoS attack.

Or

(b) Explain the plan-protect-respond-security management cycle.

14. (a) What is risk avoidance? Why does risk avoidance not endear IT security to the rest of the firm?

Or

(b) Explain how digital signatures are used for message-by-message authentication.

15. (a) Describe symmetric key encryption and the importance of key length.

Or

(b) What are virtual private networks? Describe its types.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Discuss about social Engineering in Malware in detail.

17. Explain traditional external attacks and discuss Denial of Service attack in detail.

18. Explain the types of Intrusion Detection Systems in detail.

19. Discuss the methods for evaluating security systems in detail.

20. Describe the various security mechanisms in details.

D–7048

Sub. Code
51923

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2022.

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 are the Minimum System Requirements to Install Mobile Security for Android?

2. What is Lost Device Protection in Mobile Security?

3. What is System Tuner?

4. How to Enhance the Knowledge of Mobile Security?

5. What are the Main Benefits Mobile Security?

6. What is Communication?

7. List out the Components of a wireless communication system.

8. What is Client-Server Computing?

9. What are the functions which support service and connection control?

10. What is Authentication Center (AUC)?

PART B — (5 × 5 = 25 marks)

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

11. (a) How are multiple profiles created on an Android phone?

Or

(b) How does Android support more than one user?

12. (a) Illustrate the objectives of the Bluetooth technology.

Or

(b) Why "MAC protocol designed for infrastructure based wireless network may not work satisfactory in infrastructure less environment" — Justify?

13. (a) Define the TCP issues in Mobile IP networks.

Or

(b) Summarize the advantages and disadvantages of Mobile IP.

14. (a) Compare the characteristics of cellular Communication systems.

Or

(b) What is the different malicious software's? Explain it.

15. (a) Give the advantages of mobile security.

Or

(b) Define Multiplexing. List the dimensions of multiplexing.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Describe the characteristics of a communication device.

17. Generalize the roles and application environments of mobile security.

18. Explain in detail about exploring online scheduling applications.

19. Explain the Bluetooth technology in detail with neat diagram.

20. Explain the services that are provided by the Home Agent.

———————