D–6036

Sub. Code
51911

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2024.

First Semester

CRYPTOGRAPHY AND NETWORK SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours   Maximum : 75 marks

SECTION A — (10 × 2 = 20 marks)

Answer ALL the questions.

1. Define a security attack.

2. Provide an example of a substitution technique used in cryptography.

3. Define differential cryptanalysis.

4. What are the main design principles of block ciphers?

5. What is the primary purpose of the Diffie-Hellman key exchange protocol?

6. What is the main advantages of using public-key cryptosystems over symmetric key cryptosystems?

7. What are the key components of a MAC-based hash function?

8. Write a short note on the digital signature standard.

9. What does TLS stand for in web security?

10. What is the main purpose of IP security?

SECTION B — ($5 \times 5 = 25$ marks)

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

11. (a) Develop a comprehensive model for network security and discuss its components.

Or

(b) Compare and contrast block ciphers and stream ciphers in symmetric encryption.

12. (a) Describe the role of the key schedule in the data encryption standard.

Or

(b) Discuss the significance of finite field arithmetic in the advanced encryption standard.

13. (a) Discuss the mathematical foundation of the RSA algorithm and its significance in cryptography.

Or

(b) Explain how elliptic curves are used in cryptographic algorithms to provide security.

14. (a) Explain the concept of MAC-based hash functions and how they enhance message authentication.

Or

(b) Outline the process of creating and verifying a digital signature using the EIGamal scheme.

15. (a) Discuss the differences between SSL and Transport Layer Security.

Or

(b) Explain how pretty good privacy enhances the security of electronic mail.

SECTION C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Discuss the evolution of the OSI security architecture and its impact on the development of network security protocols.

17. Explain the transformation functions used in AES encryption and decryption.

18. Discuss the role of pseudorandom number generators in asymmetric cryptographic systems.

19. Discuss the differences between MACs and digital signatures in terms of their security and applications.

20. Examine the development, implementation and significance of IP security policies in maintaining network security.

———————

D–6037

Sub. Code
51912

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2024.

First Semester

FUNDAMENTALS OF CYBER SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

SECTION A — (10 × 2 = 20 marks)

Answer ALL the questions.

1. Define cybercrime and list its types.

2. What are the tools commonly used in cybercrime?

3. What is disk forensics?

4. Explain the role of network forensics.

5. What is ethical hacking? Explain any two essential terminologies.

6. How is password hacking typically carried out?

7. What are the main difference between analog and digital evidence?

8. Why is volatile evidence important in criminal investigations?

9. What is intrusion detection? Give an example.

10. Describe what is meant by physical theft in the context of cybersecurity.

SECTION B — (5 × 5 = 25 marks)

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

11. (a) Discuss the significance of mobile forensics in modern cyber investigations.

Or

(b) Describe the process and challenges of email forensics.

12. (a) Explain network hacking and its impact on organizational security.

Or

(b) Discuss different methods of scanning in ethical hacking.

13. (a) What are the different types of digital evidence? Provide examples.

Or

(b) Discuss the rules of evidence in the context of digital investigations.

14. (a) Explain the role of anti-malware software in protecting systems.

Or

(b) Describe host-based intrusion prevention systems and their importance.

15. (a) What are the common cybersecurity vulnerabilities in system administration?

Or

(b) Explain the importance of access control in cybersecurity.

SECTION C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Compare and contrast the various types of cyber forensics, such as network forensic and malwere forensics.

17. Explain in detail the methods used in web hacking and the countermeasures that can be taken to prevent it.

18. Discuss the process of evidence collection and data seizure, and explain the challenges involved.

19. Analyze the techniques used in intrusion detection and prevention, focusing on both network-based and host-based approaches.

20. Discuss cybersecurity vulnerabilities related to poor cybersecurity awareness and propose strategies to mitigate them.

———————

D–6038

Sub. Code

51913

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2024.

First Semester

CYBER SECURITY LAW AND PRACTICE

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

SECTION A — (10 × 2 = 20 marks)

Answer ALL the questions.

1. What was the primary need for the introduction of cyber law in India?

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

3. How does the IT Act, 2000 impact the Indian law?

4. Define cyber space jurisdiction.

5. What is the significance of digital signatures in Indian law?

6. Mention any two provisions related to E-commerce in Indian law.

7. What is cyber squatting?

8. Explain the concept of reverse hijacking in trademark disputes.

9. List two examples of cyber-crimes against property.

10. Mention any one Indian case law related to cyber crime.

SECTION B — (5 × 5 = 25 marks)

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

11. (a) Discuss the amendments made to the Indian evidence Act in relation to cyber laws.

Or

(b) Explain the significance of cyber space jurisdiction with a relevant example.

12. (a) How does Indian law address the validity of E-contracts?

Or

(b) Discuss the role and functions of the cyber tribunal in India.

13. (a) Analyze the impact on intellectual property rights on the digital medium.

Or

(b) Explain the legal challenges related to domain names and trademark disputes.

14. (a) Discuss cyber crimes against individuals with relevant examples.

Or

(b) Explain the legal framework addressing crimes against the nation under Indian cyber laws.

15. (a) Provide an overview of cyber laws in the Netherlands.

Or

(b) Discuss the key features of cyber laws in Malaysia.

SECTION C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Evaluate the impact of the IT Act amendments on the Reserve Bank of India Act and bankers book evidence Act.

17. Discuss in detail the concept of E-governance and its practical implementation in India.

18. Analyze the jurisdictional challenges in trademark disputes in the digital era.

19. Examine the different types of cyber crimes in India and the legal provisions available to combat them.

20. Compare and contrast the cybercrime legislation in the United States and the United Kingdom.

———————

D–6039

Sub. Code
51921

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2024.

Second Semester

WEB APPLICATION SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours   Maximum : 75 marks

SECTION A — (10 × 2 = 20 marks)

Answer ALL the questions.

1. Mention the use of HTTP protocol.

2. Define network.

3. State the goal of Penetration testing.

4. Write the difference between pros and cons.

5. Delineate web pages.

6. Differentiate front-end development and back-end development.

7. What is denial of service?

8. Naming the common vulnerabilities in access controls.

9. How to shared hosting and application service providers?

10. List the most common web server attacks.

SECTION B — (5 × 5 = 25 marks)

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

11. (a) Discuss about the evolution of web application.

Or

(b) Differentiate client and server-side scripting.

12. (a) Describe the top five penetration testing methodologies.

Or

(b) Write short notes on (i) semantic checks (ii) handling attackers.

13. (a) Discuss the classifications of web technologies.

Or

(b) What are application maps? Which tool do you use to map an application?

14. (a) Briefly discuss authentication attacks with example.

Or

(b) Explain the following :

(i) Identifier-based functions

(ii) Multistage functions.

15. (a) Make clear to write the concept of cross-site scripting in attacking users.

Or

(b) Illuminate how application server attacking.

SECTION C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Elucidate the concept of windows and Linux, IIS and LAMP servers.

17. Explain core defences mechanism in web applications.

18. Illustrate languages, libraries and frameworks in web development technologies.

19. Describe attacking back-end components.

20. Enlighten how attacking tired application architecture.

————————

D–6040

Sub. Code

51922

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2024.

Second Semester

MALWARE ANALYSIS AND NETWORK SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

SECTION A — (10 × 2 = 20 marks)

Answer ALL the questions.

1. Differentiae between a virus and malware.

2. What is a sandbox?

3. Define branching.

4. What is meant by instruction? Provide some examples.

5. Discuss the concept packet filtering.

6. Define E-mail.

7. What is port stealing?

8. What is meant by encryption?

9. Explain the concept of cybersecurity.

10. Which operating system do you consider more secure : Linux or Android?

SECTION B — (5 × 5 = 25 marks)

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

11. (a) Differentiate between malware and spyware.

Or

(b) How can you create a fake network?

12. (a) Explain how the main method of a C program translates to assembly language.

Or

(b) Define branching statement with a suitable example.

13. (a) Discuss process monitor or process control (ProCon).

Or

(b) How would you set up Wireshark to monitor packets passing through an internet router?

14. (a) What is the function of firewall?

Or

(b) What is network sniffing?

15. (a) Discuss John the Ripper.

Or

(b) What is meant by malware, and what is the usage of malware?

SECTION C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. What are the benefits of a firewall?

17. Explain structure of virtual machine.

18. Discus the process of the X86 architecture with a neat block diagram.

19. What is an exception? Explain the types of exception.

20. What is an antivirus? Give a few examples.

———————

D–6041

Sub. Code
51923

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
DECEMBER 2024.

Second Semester

MOBILE SECURITY

(CBCS 2021 Calendar Year Onwards)

Time : Three hours Maximum : 75 marks

SECTION A — (10 × 2 = 20 marks)

Answer ALL the questions.

1. What is the different version of the Android OS?

2. Define the android framework.

3. What are the advantages of Android OS?

4. What contents are included in APK files?

5. What is coding signing?

6. Define Bluetooth.

7. What are restrict profiles?

8. Abbreviate SSL and TLS?

9. Define encryption.

10. What is ciphertext?

SECTION B — (5 × 5 = 25 marks)

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

11. (a) Explain WatsApp.

Or

(b) Write a short note on Binder IPC.

12. (a) Define dynamic enforcement.

Or

(b) Write a short note on system permission.

13. (a) What are the functions of optimized DEX?

Or

(b) Which system settings are displayed in the wireless and network section?

14. (a) Discuss symmetric encryption.

Or

(b) Define public key infrastructure.

15. (a) What is a digital certificate?

Or

(b) What is a credential used ID?

SECTION C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. How does the android system protect against malicious applications?

17. What is permission enforcement? Explain their types.

18. Discuss in detail packet verification.

19. Explain external storage in Android OS.

20. What is the difference between public key and private key?