D–5043

Sub. Code
51911

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
MAY 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 symmetric and asymmetric encryption.

2. Define cryptography.

3. Define security mechanism.

4. Define steganography.

5. Why network need security?

6. Define Encryption.

7. Define confidentiality and authentication.

8. What are roles of public and private key?

9. What is message authentication?

10. Give the benefits of IP security.

PART B — (5 × 5 = 25 marks)

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

11. (a) How key can be distributed in Cryptography? What are the issues?

Or

(b) What is Encryption and Decryption? What is Active and Passive attacks?

12. (a) What types of attacks are addressed by message authentication?

Or

(b) Discuss about the Confidentiality, Integrity and Availability in detail.

13. (a) Difference between Private Key and Public Key Algorithm.

Or

(b) Write the principles of public key Cryptography.

14. (a) What are two common techniques used to protect a password file?

Or

(b) How to secure hardware, secure software and an efficient legal system.

15. (a) Write the firewall design principles.

Or

(b) Explain the types of Intrusion detection systems.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions

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

17. Explain RSA algorithm and give example of generation of public and private keys and generation of cipher text through RSA.

18. Why is Asymmetric Crytography bad for huge data? Specify the reason in detail.

19. Evaluate the authentication protocol and list its limitations, how the limitations overcome

20. Explain the network security model and its important parameters with a neat block diagram.

————————

D–5044

Sub. Code
51912

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
MAY 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. Why is cyber security important?

2. Define CIA?

3. Define Virus, Worms and Torjan Horse?

4. Define Vulnerability.

5. Write short notes about Threads.

6. Define Cyber Crime?

7. Write short notes on Cross Site scripting.

8. Define vulnerability and risk.

9. Define Salami Attack.

10. Define Cyber Stalking.

PART B — (5 × 5 = 25 marks)

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

11. (a) Compare and explain about web-based attacks and system-based attacks in detail.

Or

(b) What is World Wide Web? Explain.

12. (a) What is password manager? How does it work? List some of the popular password managers.

Or

(b) State four types of problems due to installation of unauthorized software.

13. (a) Define virus and describe the virus spreading mechanism.

Or

(b) What is Wireless LAN? How to secure wireless network infrastructure?

14. (a) Explain some of the tips for email security in detail.

Or

(b) Discuss about intrusion detection system and intrusion prevention system compare and give its importance.

15. (a) Give four examples of computer intrusion in detail.

Or

(b) Explain sniffing and spoofing with suitable example.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions

16. Give four criteria's used for password management.

17. Describe how the various types of fire walls interact with the network traffic at various levels of the OSI model.

18. How a network based IDPS differ does from a host based IDPS example?

19. List and describe the options available for the location of the information security functions within the organization. Discuss the advantages and disadvantages of each option.

20. Discuss any three crytographic tools and their significance in information security.

———————

D–5045

Sub. Code
51913

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
MAY 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 space.

2. What is cyber law? Write its advantages and disadvantages?

3. Write about understanding of cyber space.

4. Define cyber law and cyber space.

5. Write short notes interface of technology in cyber space.

6. Write short notes law defining cyber laws.

7. What is jurisdiction in cyber space?

8. What are the concept of jurisdiction and its types?

9. What is internet jurisdiction?

10. Write short notes on Indian context of jurisdiction.

PART B — (5 × 5 = 25 marks)

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

11. (a) Explain in detail the public key functioning and protection provided by it under the electronic signature.

Or

(b) Define the term 'passive advertisement' and explain the issues involved in regulation of internet advertising.

12. (a) Explain the provisions for protection of online Trade Marks under the Trade Marks act, 1999.

Or

(b) Explain the provisions relating to infringement of intellectual property rights.

13. (a) Define the term 'Hacking' and explain its essentials.

Or

(b) Explain justice dispensation system for cyber crimes.

14. (a) Discuss how industrial Designs created with the use of cyber technology can be protected in the light of the Designs Act.

Or

(b) Examine the concepts of data file sharing technology in peer-to-peer networks and implication on cyber copyrights.

15. (a) Examine the method of dealing with cyber-squatting of domain names and the resulting disputes under the Trade Marks Act, 1999.

Or

(b) Discuss whether various international treaties and conventions have been instrumental in defining the path of intellectual property rights in the cyber world.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions

16. What is computer networking? Explain the functioning of VoIP as a communication technique in the cyber space.

17. What is called 'Domain Name' and explain with the help of case laws the regulation of domain names in the Indian legal system?

18. What is internet protocol services? Explain its effectiveness and utilization in the cyber crime investigation.

19. Define the term 'cyber squatting' and what kinds of protection available to the consumers in the cyber world against it?

20. Answer any four of the following:

    (a) Electronic records retention

    (b) Data protection

    (c) Consumer protection in cyber world

    (d) Trans-national data flow

    (e) Virtual banking operations

    (f) Public key infrastructure.

D–5046

Sub. Code

51921

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION, MAY 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 Web application security?
2. What is the difference between authenticaion vs authorization?
3. What is “Vulnerability"?
4. What threat arises from not flagging HTTP cookies with tokens as secure?
5. How can we protect web applications from forced browsing?
6. Difference between penetration testing and other forms of security testing.
7. List out any five WAS Vulnerabilities.
8. Mention the controls to test during the assessment.
9. Define URN.
10. What is the basic design of WAS?

PART B — (5 × 5 = 25 marks)

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

11. (a) What do you see as the most critical and current threats effecting internet accessible web sites?

Or

(b) What are the essential requirements of effective access control?

12. (a) Describe how the database servers be protected against the attacks on web.

Or

(b) How can we detect the real IP address of an attacker?

13. (a) What is server hacking? Explain.

Or

(b) What does secure by default mean in Web security?

14. (a) What are the security features being provided in Web security?

Or

(b) What are the most important steps you would recommend for securing a new web application.

15. (a) Discuss about online resources do you use to keep abreast of web security issues?

Or

(b) List out some examples of a recent web security vulnerability or threat? Explain.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions

16. Different approaches are used for handling user input in web applications. Explain.

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

18. Discuss some of the common vulnerabilities with respect to access control.

19. Describe how source code disclosure can be effectively used to safeguard against the vulnerabilities in applications.

20. Discuss about the database vulnerabilities. Discuss some mechanisms to handle it.

D–5047

Sub. Code
51922

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION,
MAY 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. Define the term thread environment

2. Define integrity.

3. Define Cipher text.

4. What is VPN?

5. Define Virus.

6. What is XSS?

7. What do you mean by Malware writers?

8. Define cryptography.

9. What is a Host?

10. Who are all called cyber attacker?

PART B — (5 × 5 = 25marks)

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

11. (a) Explain how to secure Ethernet networks?

Or

(b) Explain the firewall architecture.

12. (a) Explain the process of securing e-mail.

Or

(b) What is a vulnerability? How to manage vulnerabilities? Explain.

13. (a) What is IT disaster recovery? Explain the different types of backup facilities.

Or

(b) How to evaluate the security systems? Explain.

14. (a) Distinguish between credit card theft and identity theft in detail.

Or

(b) How do criminals usually get the information they need for credit card theft and identity theft?

15. (a) Discuss about authentication in detail.

Or

(b) Illustrate data protection: Backup and Policies.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions

16. Describe the intrusion response process for major incident in detail.

17. What are the threads in India for cashless money transaction? How to secure our online money transactions?

18. What is the need of disciplined security management process? Explain the plan – protect – respond cycle.

19. How to evaluate the security systems? Discuss with example.

20. What are the problems with classic risk analysis calculation?

———————

D–5048

Sub. Code
51923

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY EXAMINATION, MAY 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. Which is latest version of Android OS?

2. What is android?

3. Define mobile security.

4. Write note on antennas and wave propagation.

5. Define GPRS?

6. Define the term wireless?

7. Difference between wired and wireless networks.

8. What is the need for mobile security?

9. What is multi user in mobile phone?

10. What is authentication center (AUC)?

PART B — (5 × 5 = 25 marks)

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

11. (a) Write a note on android device available in market.

Or

(b) Explain android perspectives in detail.

12. (a) How are multiple users supported in android automotive?

Or

(b) Discuss the different threats to wireless networks.

13. (a) Explain the lifecycle methods involved in the android activity?

Or

(b) What are the different types of services in android?

14. (a) Explain about various wireless privacy challenges.

Or

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

15. (a) Explain android architecture briefly in detail.

Or

(b) Explain the security issues in android in detail.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions

16. What are the core components under the android application architecture? Explain any two in detail.

17. Describe the list the different versions of android in detail.

18. Explain with diagram the android platform architecture in detail.

19. Compose the solutions for security issues in mobile OS in detail.

20. Write about mobile security in detail and give working principles of mobile security. Give some advantages and disadvantages of mobile security.