D–7127		Sub. Code
		51911

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY

EXAMINATION - MAY 2021

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.   What are the three aspects of security?

2.   Define Brute-force attack.

3.   Mention the different modes of operation in DES.

4.   What is the difference between diffusion and confusion?

5.   Define cryptography.

6.   Whether the Diffie Hellman key exchanges protocol is vulnerable?

7.   Name the classes of message authentication function.

8. Specify the basic task for defining a security service.

9. Draw the diagram for PGP message transmission reception.

10. Define PGP Services.

PART B — (5 × 5 = 25 marks)

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

11. (a) Explain classical Encryption Techniques.

Or

(b) Differentiate symmetric and asymmetric encryption.

12. (a) Discuss in detail

(i) Finite Field Arithmetic (ii) AES Structure.

Or

(b) Compare stream cipher with block cipher with example.

13. (a) Differentiate in detail about public key and conventional encryption.

Or

(b) How pseudorandom number generation based on asymmetric cipher?

14. (a) What are the requirements of Message Authentication? Discuss.

Or

(b) Explain MAC based Ciphers.

2 **D–7127**

15. (a) How Digital signature differs from authentication protocols?

Or

(b) Discuss in detail about Digital Signature Standard.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Describe the various security mechanisms.

17. Explain in detail about AES.

18. Discuss Diffie-Hellman Key Exchange algorithm with its merits and demerits.

19. Describe about Hash Function. How its algorithm is designed? Explain its features and properties.

20. Write down the steps involved in Elgamal DSS and Schnorr DSS? Explain.

_____

D–7127

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY
EXAMINATION - MAY 2021

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 are the Computers Crime?

2.   Differentiate Bitcoin and Blockchain.

3.   Define Malware Forensics.

4.   Write the expansion of ISAKMP Explain.

5.   Name the hacking operating systems.

6.   Define Ethical hacking. List its limitations.

7.   Why collect Evidence.

8.   What is Volatile Evidence?

9.   Define vulnerabilities.

10.   What are the five elements of theft?

PART B — (5 × 5 = 25 marks)

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

11. (a) Illustrate the Classification of Cyber Criminals.

Or

(b) What are the Challenges available in Cyber Crime? Explain.

12. (a) Do you think data recovery is the main role in computer forensics. Justify your answer. Explain in briefly.

Or

(b) (i) Write short notes on computer forensics services.

(ii) Describe about computer forensics fundamental.

13. (a) Explain about some hacking applications with an example.

Or

(b) How will you crack the Password? Elaborate the steps in details.

14. (a) Enlighten the following terms:

(i) Data viewing

(ii) Keyword searching

(iii) Decompressing

Or

(b) Enumerate the guidelines for seizing digital evidence at the scene.

2 **D–7128**

15. (a) Discuss in detail Host based Intrusion Prevention.

Or

(b) Give explanation of Weak Authentication and Cyber Security Safeguards.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. How does a computer become infected with Ransom ware? How you protect against Ransom ware? Explain.

17. Why should the computer incident or crime scene be secured? Who is responsible for securing the scene? Explain.

18. Discuss in detail about Network Hacking and Web Hacking.

19. What is digital evidence? State and explain general tasks that the investigators perform when working with digital evidence.

20. Explicate Network based Intrusion detection systems and Network based Intrusion Prevention systems.

_____

D–7128

D–7129

DISTANCE EDUCATION

DIPLOMA IN CYBER SECURITY.

EXAMINATION - MAY 2021

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.   What is Cyber Space?

2.   What is Phishing?

3.   Why we need Cyber Law?

4.   What is Hacking?

5.   What is benefits of E-Governance?

6.   What is Digital signature?

7.   Define Trademark?

8.   Define Patent?

9.   What do you mean by Cyber Crime?

10.   List out any two Cyber Crime Penalties?

PART B — (5 × 5 = 25 marks)

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

11. (a) Give a brief overview about Cyber Law?

Or

(b) Write short notes on the various Authorities under IT Act and their powers?

12. (a) Give an overview of Amendments to Indian Penal code?

Or

(b) Explain about Reserve Bank of Indian Act?

13. (a) Write about the role of Digital Signature in Indian Lows?

Or

(b) Explain about the E-Governance concept and practicality in India?

14. (a) Briefly Explain about the Domain names and Trademark disputes?

Or

(b) Explain about Copyrights in Computer Programs?

15. (a) Write short notes on Crime against Property?

Or

(b) Briefly Explain about Crime against Nation?

2 **D–7129**

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. Discuss about the Amendments passed in Cyber Law?

17. Discuss in detail about Cyber Space Jurisdiction?

18. Explain about the Taxation issues in Cyberspace?

19. Discuss about Jurisdiction in Trademark Disputes?

20. How do countries like UK and Australia fight against Cyber Crime?

————————

D–7129