Instructions:

This assignment consists of three parts: theoretical questions, practical exercises, and a research component. Please adhere to the following guidelines:

Provide clear, concise answers and explanations.

For practical exercises, include code snippets, diagrams, or screenshots as needed.

Cite any external sources or references used.

Submit your assignment as a single PDF document.

1. Part 1: Theoretical Questions (40 Marks)
    - Network Security Principles (20 Marks)
    - Describe the primary objectives of studying network security. (5 Marks)
    - Explain the OSI Security Architecture and its importance in network security. (5 Marks)
    - Discuss the differences between passive and active security attacks and provide examples of each. (10 Marks)
    - Cryptography Basics (20 Marks)
    - Define cryptography and its role in securing information. (5 Marks)
    - Compare and contrast symmetric and asymmetric encryption methods. Provide examples of algorithms used for each. (10 Marks)
    - Explain the concept of non-repudiation and its significance in digital communications. (5 Marks)
2. Part 2: Practical Exercises (30 Marks)
    - Implementing Cryptographic Algorithms (15 Marks)
    - Write a simple program in Python to implement the Caesar cipher for encrypting and decrypting a text message. (7 Marks)
    - Demonstrate the use of a public-key cryptography algorithm (e.g., RSA) to encrypt and decrypt a message. You may use a cryptographic library. (8 Marks)
    - Network Security Simulation (15 Marks)
    - Using a network simulation tool (e.g., GNS3, Packet Tracer), design a basic network topology that includes a firewall and a VPN. Explain how data is secured when transmitted across this network. (15 Marks)
3. Part 3: Research Component (30 Marks)
    - Cryptography Chapter Proposal Analysis (30 Marks)
    - Review the provided chapter proposal on cryptography. Critically analyze the proposed topics, suggesting at least two additional areas or technologies that should be included in the chapter. Justify your choices based on current trends and the importance of these areas in the fields of network security and cryptography.
    - For the research component of your assignment, consider analyzing how the chapter addresses the balance between technical depth and accessibility for readers, the inclusion of historical context to enrich understanding, and whether the chapter could benefit from more examples of real-world application of cryptographic principles. Additionally, explore current trends not covered in the chapter, such as advancements in blockchain technology, the implications of quantum computing on encryption, and emerging standards in cryptographic security.
    - Use the reference book for this class as guidance for your analysis.