Encryption Methods Analysis Writing Task

In this assignment, you will analyze different encryption methods, demonstrate your understanding of how they work, and evaluate their effectiveness for various applications. This task will help you develop a deeper appreciation for the mathematical foundations of cryptography and their real-world implications.

The Assignment

Part 1: Understanding Symmetric-Key Encryption

Choose ONE of the following symmetric-key encryption scenarios to analyze:

A. **Scenario A: Substitution Cipher**
   Analyze the security of a substitution cipher where each letter of the alphabet is replaced by another letter according to a fixed pattern.
   1. Create a specific example of a substitution cipher (not a simple Caesar shift) and use it to encrypt a short message of at least 20 characters
   2. Explain how your cipher works and show the encryption/decryption process step-by-step
   3. Discuss at least two vulnerabilities of this cipher and explain how they could be exploited
   4. Suggest at least one improvement that would make this cipher more secure

B. **Scenario B: Transposition Cipher**
   Analyze a keyword-based columnar transposition cipher.
   1. Select a keyword and use it to encrypt a message of at least 20 characters using the columnar transposition method
   2. Show your work step-by-step, clearly demonstrating how the message is arranged in the grid and how the columns are ordered based on the keyword
   3. Explain how someone would decrypt your message if they knew the keyword
   4. Discuss why this method is more secure than a standard row-by-column transposition without a keyword

Part 2: Public Key Cryptography Analysis

For this part, explain the Diffie-Hellman-Merkle key exchange process using your own small example:

1. Select small values for the shared prime number p and generator g
2. Choose secret values for both parties

3. Walk through the complete key exchange process step-by-step, showing all calculations
4. Explain what information would be visible to an eavesdropper and why they couldn't determine the shared secret key
5. Discuss at least one real-world application where this key exchange method is valuable

Part 3: Comparative Analysis

In 2-3 paragraphs, compare symmetric-key and public key cryptography by addressing the following:

1. Identify at least three key differences between symmetric-key methods and public key cryptography
2. Analyze the computational efficiency of both approaches - which is faster and why?
3. Explain which approach is more secure and under what circumstances
4. Describe a practical system that uses both methods together and explain why this combination is beneficial
5. Discuss how quantum computing might affect the security of both approaches in the future

Your submission should include:

- Complete solutions for Parts 1 and 2 with all work shown
- Clear explanations of the mathematical processes involved
- Thoughtful analysis in Part 3 that demonstrates understanding of both encryption approaches
- Proper terminology throughout

This assignment is worth 20 points. Your work will be assessed on mathematical accuracy, clarity of explanations, depth of analysis, and understanding of cryptographic principles.

Rubric:

Criteria	Proficient	Developing	Not Evident	Points
Symmetric-Key Encryption Analysis	Correctly implements chosen cipher with clear step-by-step work. Thorough explanation of encryption/decryption process. Insightful discussion of vulnerabilities and improvements that demonstrates deep understanding.	Cipher implementation contains minor errors. Explanation is mostly clear but may lack detail in some areas. Discusses basic vulnerabilities but analysis could be deeper.	Significant errors in cipher implementation. Unclear or incorrect explanation of process. Minimal or inaccurate discussion of vulnerabilities.	___/6
Public Key Cryptography Example	Complete and accurate demonstration of Diffie-Hellman-Merkle key exchange with all calculations shown. Clear explanation of why the system is secure against eavesdroppers. Thoughtful application example.	Diffie-Hellman-Merkle example has minor computational errors. Explanation of security is generally correct but may lack precision. Application example is present but lacks depth.	Significant errors in key exchange calculations. Explanation of security is missing or fundamentally flawed. Application example is inappropriate or missing.	___/7
Comparative Analysis	Thorough, accurate comparison of encryption approaches that addresses all required elements. Demonstrates sophisticated understanding of efficiency, security tradeoffs, and future implications. Practical application example is relevant and well-explained.	Comparison addresses most required elements but may lack depth in some areas. Shows basic understanding of differences but may oversimplify some aspects. Practical application example is somewhat relevant.	Comparison is superficial or contains significant misconceptions. Missing multiple required elements. Practical application example is irrelevant or missing.	___/7

Total				___/20