Assignment 13: Data Security, Data Privacy, and Data Governance

Data Engineering Practices and Principles

Part 1: RSA Encryption and Decryption (50 points)

Objective: The first part of this assignment is to introduce students to the concept of public key cryptography and to test their understanding of RSA encryption and decryption.

Instructions:

1. You will be given a private key and an encrypted message. Use Python to decrypt the message using the private key.
2. You will be given another message that was encrypted using AES symmetric encryption. You will need to decrypt the message using the nonce, key, and encrypted message.
3. The data for each of the messages can be found in the assignment ZIP file.
4. You are allowed to use any code you find on the internet or elsewhere to solve these problems.
5. Submit your solution code along with a brief explanation of your approach and any references used.

Part 2: Essay (50 points)

Objective: The second part of this assignment is to demonstrate your understanding of data security, data privacy, and data governance by comparing and contrasting the strengths and weaknesses of RSA and AES encryption.

Instructions:

1. Write a 1,000 word essay explaining the pros and cons of each encryption regarding data security, data privacy, and data governance.
2. Start with an introduction to the concepts of data security, data privacy, and data governance. Explain their importance and the challenges they pose.
3. Provide a brief overview of RSA and AES encryption. Explain the strengths and weaknesses of each encryption method.
4. Compare and contrast the two encryption methods in terms of their effectiveness in protecting data security, data privacy, and data governance. Provide examples where applicable.
5. Discuss the potential impact of each encryption method on data governance. Explain how each method can help or hinder compliance with data governance regulations.
6. Conclude your essay with your overall assessment of the strengths and weaknesses of RSA and AES encryption and their suitability for data security, data privacy, and data governance.
7. Use at least three credible sources to support your arguments. Include proper citations and references.

Submission Guidelines:

1. Submit your solution code and essay as three separate files:
   1. <student-first-intial><student-last-name>-RSA\_solution.ipyn
   2. <student-first-intial><student-last-name>-AES\_solution.ipyn
   3. <student-first-intial><student-last-name>-essay.pdf (or .docx)
2. Use proper formatting and citation styles for your essay.
3. Submit your files in PDF or Word format.

Grading Criteria:

1. Correctness of the solution code (25 points)
2. Clarity and thoroughness of the solution explanation (10 points)
3. Quality of the essay content (40 points)
4. Quality of the writing (10 points)
5. Proper formatting and citation (5 points)