Final Project: Creating an Encryption System

1 Description of the project

Summary

For this project, you will be creating your own encryption system. Then you will use your encryption system to encrypt several messages of various lengths. You will write out instructions for decrypting your message and test these out on a friend.

1.1 Creating a 2-step Encryption System

1. **Create an encryption system that involves at least 2 steps**. Here are the requirements:
   (a) One step must be a **substitution cipher**, meaning that you are replacing the characters in your message with different characters, following some established mapping (such as an alphanumeric Caesar cipher with a given shift).
   (b) One step must be a **transposition cipher**, meaning that you are changing the order of characters to obscure the message (such as tabular transposition).
   (c) Each step needs to be compatible with numerical digits as well as English letters.
   (d) Each step need to be **reversible**, meaning that you can write down a step-by-step process to decrypt a message.
2. **Give your encryption system a name**.
3. **Write out an explanation of both encryption steps**. Use words and terms that someone who is not in the class would be able to understand.
4. **Write out a step-by-step guide for decrypting a message with your system**. Use words and terms that someone who is not in the class would be able to understand and apply.

Encrypting Messages

1. **Test your encryption system by encrypting the following three short messages:**.
   (a) Encrypt the word **PASSWORD**.
   (b) Encrypt the phrase **THANK YOU FOR YOUR HELP**.
   (c) Encrypt the number **9074747332**.
2. **Create a long message** in English of at least 50 words. Feel free to use a famous quote, a song lyric, a message of your own, or anything else, so long as it is coherent English.
3. **Use your encryption system to encrypt the long message you just created**.

Further Analysis

1. **Test your encrypted system with a friend** by providing your decryption instructions and your three encrypted short messages (not the long one). See if they can decode them.
2. **Answer each of the following questions:**
   (a) How did your friend do? Were your decryption instructions clear enough?
   (b) How hard do you think it would be for someone to decrypt these messages without knowing your encryption process? Is your encryption system secure?

2 Project Deliverables

How to submit

- Your project must have a **Title Page**, containing your name and which project you are completing.
- Your final project must be submitted in class during the final exam period. (Note that you can print out materials at the Student Success Center!)
- Your final project must be typed.
- You should use sentences to describe what each piece of your project is doing and what you are computing: one of your classmates should be able to read your project and understand what you are doing.
- Your final project must be stapled together.

What to submit

Your final project will have three sections. Each section should start on a separate page.

- A section titled **My Encryption Method** containing:
  - The name of your encryption system
  - The explanation of both steps of your encryption process
  - A step-by-step guide for encrypting a message with your system
  - A step-by-step guide for decrypting a message with your system
- A section titled **Encrypted Messages** containing:
  - The encrypted form of the word PASSWORD
  - The encrypted form of the sentence THANK YOU FOR YOUR HELP
  - The encrypted form of the number 9074747332
  - Your long encrypted message of at least 50 words.
  - On a separate page, your original unencrypted long message.

- A section titled **Further Analysis** containing
  - Your answer to the question:

    "How did your friend do? Were your decryption instructions clear enough?"
  - You answer to the question:

    "How hard do you think it would be for someone to decrypt these messages without knowing your encryption process? Is your encryption system secure?"

3 Grading

Your project will be graded out of 100 points using the following rubric:

1. Your encryption system (15 points)
   (a) A clear description of your substitution
   (b) A clear description of your transposition, including a key word and its use
   (c) A clear description of how to encrypt a message using your system
   (d) A name for your encryption system
   (e) A system understandable by someone who is not in Math F113X
   (f) An encryption system compatible with numbers and letters
2. Your encrypted messages (15 points)
   (a) Correct encrypted form of the word PASSWORD
   (b) Correct encrypted form of the sentence THANK YOU FOR YOUR HELP
   (c) Correct encrypted form of the number 9074747332
   (d) A long encrypted message of at least 50 words.
   (e) The original unencrypted (plain text) long message, on a separate page.
3. Decryption check (20 points)
   (a) A clear description of how to decrypt your messages
   (b) A step-by-step guide for decrypting messages understandable by someone who is not in Math F113X
   (c) Encryption and decryption instructions such that the grader can successfully implement.
4. How did your friend do? (20 points)
   (a) Explain whether or not your friend successfully decrypted all three short messages using the step-by-step decryption guide.
   (b) State how long it took your friend to decrypt your messages

(c) Assess the clarity of your step-by-step decryption guide and describe how it could be improved.

5. Answer to "How hard do you think it would be for someone to decrypt these messages..." (20 pts)
   (a) Provide an analysis of your encryption system
   (b) Talk about at least one strength of your encryption system that would make it difficult to hack
   (c) Talk about at least one possible weakness of your encryption system that may make it vulnerable to hacking
   (d) Give an overall assessment of the security of your encryption system's security
6. Grammar, mechanics, and following directions (10 points)
   - Use sufficient words and **complete sentences** in your discussions
   - Use correct grammar and mechanics in your writing
   - Use words and headings to make it clear what you are answering where
   - Computations should be presented clearly and legibly
   - Follow the directions