Final Project: Encryption

Math F113X: Math and Society

Overview

Choose a plaintext and encrypt it using our three standard ciphers, then **design** your own two-step encryption system and apply it to the same plaintext, and finally **analyze** the usability and security of your system by testing it with a friend.

Your final submission must be typed, stapled, and organized into clearly labeled sections as outlined in the checklist below. Write in complete sentences throughout, providing sufficient background and detail so that a classmate could follow your work. Explanations of your encryption and decryption steps should be understandable by someone who has not taken Math F113X. Use the rubric and checklist to guide your decisions.

Use of AI

The use of AI (ChatGPT, Claude.ai, etc.) to produce or edit any part of your project is prohibited and will result in a grade of zero.

Submission Checklist

Complete all of the following. Each item should appear as a clearly labeled section in your report.

☐ **Title page:** Include your name and the project title.

Section 1: Standard Ciphers

☐ **Plaintext:** State your plaintext (at least 50 characters).

☐ **Shift cipher:** State your Caesar shift (prohibited: 0, +1, −1). Show the encrypted result.

☐ **Keyword:** State your keyword (at least 5 letters). Use it for both ciphers below.

☐ **Transposition cipher:** Encrypt your plaintext using tabular transposition with your keyword. Include supporting work.

☐ **Vigenère cipher:** Encrypt your plaintext using your keyword. Include supporting work.

Section 2: My Encryption Method

☐ **Name:** Give your two-step encryption system a name.

☐ **Substitution step:** Describe your substitution cipher clearly. It must differ from the shift cipher used in Section 1.

☐ **Transposition step:** Describe your transposition cipher clearly. It must use a different keyword than the one used in Section 1.

☐ **Encryption instructions:** Provide a step-by-step guide for encrypting a message with your system.

☐ **Decryption instructions:** Provide a step-by-step guide for decrypting a message with your system, written so that someone outside this class could follow it.

☐ **Apply your method:** Encrypt your plaintext using your system. Include supporting work.

☐ **Friend test:** Give a friend your ciphertext and decryption guide. Include the materials associated with the Friend test in the appendix.

Section 3: Analysis

☐ **Usability analysis:** In 1–2 paragraphs, describe your friend test: what happened, whether your friend succeeded, and how long it took. Assess the clarity of your decryption guide and suggest improvements. Conclude with an overall judgment of how practical your encryption method is for a novice user.

☐ **Security analysis:** In 1–2 paragraphs, discuss at least one strength and one weakness of your encryption system, then give an overall assessment of its security.

Appendix

☐ **Friend's Work:** Attach the materials you gave to your friend and your friend's decrypting work.

Rubric

Component	**Description**	**Points**
Standard ciphers	plaintext, shift, and keyword stated	25
	shift cipher correctly applied	
	transposition cipher correctly applied, with supporting work	
	Vigenère cipher correctly applied, with supporting work	
My Encryption Method	system named	25
	substitution and transposition steps clearly described	
	clear encryption and decryption instructions	
	method correctly applied to plaintext, with supporting work	
Friend test	process described; outcome and time reported	20
	clarity of guide assessed with suggestions for improvement	
	all associated materials included in appendix	
Analysis	usability discussed	20
	security discussed	
Overall composition	Quality of writing, organization, and following directions	10
Total		**100**