CHARLESTON SOUTHERN UNIVERSITY

Project 2 CSCI 452/552

Department of Computer Science

Objective

This project is designed to help you understand how encryption and decryption work. It is structured as a group project for undergraduate students and as an individual project for graduate students. All students must submit a lab report to Blackboard that includes demo videos and detailed project report.

You may use any programming or scripting language (e.g., Java, C++, Python, Perl, etc.) to complete the tasks under Ubuntu (no other OS is allowed).

By the end of this lab, you should be able to:

- Encrypt a message.
- Decrypt a message.
- Break an encrypted message.

Demonstration Requirements:

- Choose a statement from John Chapter 1, then encrypt and decrypt it. After completing your encryption and decryption demos, you will exchange one of your encrypted ciphertexts with another group for them to attempt to crack. Please refer to the accompanying handout for further instructions on completing each task.

Task I. (40%) The Caesar Cipher

In this task, you will make a Caesar cipher according to what you have learned in class. We will use the formula of $c_i=E(p_i)=p_i+\text{offset}$. You can choose your own offset.

1. Create a program/script to encrypt a message. Demo how to accept a random plaintext, encrypt the plaintext and show the ciphertext.
2. Create a separate program/script to decrypt the ciphtertext. Demo how to accept a random ciphertext, decrypt the ciphertext and show the plaintext.

Task II. (40%) Columnar Transpositions

In this task, you will make a Columnar Transpositions cipher according to what you have learned in class. We will choose to use 6 columns instead of 5 columns in this project.

1. Create a program/script to encrypt a message. Demo how to accept a random plaintext, encrypt the plaintext and show the ciphertext.
2. Create a separate program/script to decrypt the ciphtertext. Demo how to accept a random ciphertext, decrypt the ciphertext and show the plaintext.

Task III. (20%) Cryptoanalysis

In this task, you will use cryptoanalysis learned in class and break one of the encryptions of other team. You will create a workable encryption and decryption program. Use your encryption application to encrypt a verse from John 1. Encrypt your message and post to Blackboard discussion forum for other teams to see. Limitations are:

1. You are going to use a *mix of both* encryptions.
2. You cannot use other encryptions.
3. The “rounds” of encryption is no more than 3 rounds.
4. Your plaintext message must be a verse from John 1.

How this task is graded:

1. Turn in your algorithm and your plaintext for all tasks. Failed to do will cost your team 40 points
2. Every message you decrypt will earn your team 20 points, you can earn a maximum of 40 points.
3. If your team’s cyphertext is cracked by other teams, you will lose 20 points.
4. Only the first team who cracks a ciphertext will earn the credit.
5. You must post how you crack other team’s code in the forum.
6. The maximum number of points is no more than 100 points for this project.