CS 378 - Spring 2016	Assignment 2 - Code Breaking
System Security (Freshman Research Initiative)	**Due: Feb 15th and 22nd at 11:59pm**

Assignment Objectives

In this lab, you will execute a chosen-plaintext attack on two encryption algorithms. A chosen-plaintext attack lets the adversary choose the encryption algorithm's input and observe the generated encrypted text. The goal of the adversary is to reverse-engineer the encryption algorithm.

Lab tasks

The lab is divided into three major tasks. For the first task, you should reverse-engineer two encryption algorithms. For the second task, you should design and implement a relatively secure encryption algorithm (more guidelines given later). For the third task, you should reverse-engineer an encrypted algorithm created by another team in the class.

Task 1: Reverse-engineer the encryption algorithm. Reverse-engineer the encryption algorithm used by the programs given to you. You will need to be creative in designing inputs to the program. Form hypotheses, and test them by crafting different inputs.

The two encryption programs are available at the following URLs:
`cs.utexas.edu/users/fri-security/enc-lab/p1/?q=Howdy!`
`cs.utexas.edu/users/fri-security/enc-lab/p2/?q=Howdy!`

Please replace the string `Howdy!` with any input of your choice.

Deliverables: Please turn in a report that briefly explains the steps you took to reverse-engineer the algorithm.

Task 2: Designing and implementing your own encryption and decryption algorithms. Try your hand at designing encryption and decryption algorithms! Now that you've seen two examples, devise an algorithm that does not have the same weaknesses. You may implement your algorithm in Java, C, or C++.

There are two restrictions for your algorithms:

- You should design your algorithms completely on your own. Use of cryptographic library functions is not permitted. You are also not permitted to find an algorithm on the Internet and implement it as your project.
- You should implement a stream cipher, and not a block cipher.

Please do not discuss the design of your encryption algorithm with classmates other than your partner!

Deliverables: Please turn in the source code for your encryption and decryption algorithms with 3 inputs and outputs.

Tasks 1 and 2 are due on Monday, February 15 at 11:59 pm on Canvas.

Task 3: Reverse-engineer another team's encryption algorithm. You will be randomly assigned another team's encryption algorithm. Reverse-engineer the encryption algorithm using the techniques that you have learned from earlier parts of this assignment.

Deliverables: Please turn in a short report describing the encryption algorithm and the steps you took to try to reverse-engineer the algorithm. Illustrative examples are encouraged.

Task 3 is due on Monday, February 22 at 11:59 pm on Canvas.