Final Project Design Document:

Encrypting Machine

by **Carlos Rubio** and **Stephanie Gregory**

*CS2810-002: Introduction to Computer Architecture*

**Dr. L. Roy Thackeray**

# Introduction

This document contains a formal proposal for the final project of the CS2810-002 class by Dr. L. Roy Thackeray. During the course of the semester, we’ve been learning the principles of computer architecture and how are the instructions given by the users processed and stored. The purpose of the final project is to apply the gained knowledge into a program written for LC3 ISA and demonstrate mastery over the concepts of project design, ISA, Assembly Language, and so forth.

# Project Description

**This proposal is for a program that can generate an encrypted message in Caesar’s cipher system based to certain parameters**, including the integer from 1 to 26 that represents the key and a string of ASCII uppercase characters which represents the message. The supported encrypting system is Caesar’s Cipher.. **The program will consist of a main loop in which the user can input some basic parameters, and then one of the many subroutines will start, returning and exporting an encrypted message.**

# Background and Problem Statement

I’ve always been akin to cryptography: I find it’s systems fascinating, and a very engaging puzzle to work with. In these days, with the raise of Cybersecurity, understanding and deploying methods of encrypting data is ever more important. This project will suppose a first step for me in understanding this systems better.

# Applications

This project is done mainly for academic interests, and its source code will be written in the hypothetical with LC3’s ISA in mind. Therefore, *there are not real expected applications*. However, if given the possibility, **this system could be used to protect messages over the internet as well as within the equipment.** As stated before, this is very crucial in a time where data privacy and security is important and cyberattacks happen often and might endanger others.

# Project Goals

1. Understand the principles of computer architecture.
2. Study and comprehend the LC3 ISA.
3. Write a complete program in Assembly Language.
4. Master project planification and design, using tools such as flowcharts and pseudocode.
5. Understand classic encryption codes.
6. **Create a versatile encrypting program.**

# Time Line

* Proposal: **March 8th, 2024**
* Design Document: **March 25th, 2024**
* Program Submission: **April 23rd, 2024**

Encrypting Machine

Design and Features

# Description

1. A routine that can generate an encrypted message in Caesar’s cipher system based to certain parameters, including the integer from 1 to 26 that represents the key and a string of ASCII uppercase characters which represents the message. The supported encrypting system is Caesar’s Cipher. The program will consist of a main loop in which the user can input some basic arguments, and then one of the many subroutines will start, returning and exporting an encrypted message.

# Feature descriptions

1. Selection of one of two modes based on Caesar’s Cipher: an encryption mode that adds a positive key to an ASCII string, and a decryption mode that subtracts a positive key to an ASCII string.
2. The program will work on a loop, allowing multiple consecutive sessions.
3. The program error proves the input parameters and avoids unsupported arguments (Goose Typing)
4. The program handles strings of ASCII uppercase and whitespace (Space) characters properly.
5. The program handles ASCII numeric strings with with variable number of characters (digits) and converts properly them to binary for easy integer-binary arithmetic.

# User Interface (Command Line Interface)

## Welcome

|=============================|   
| Caesar’s Code Machine |  
| by Carlos Rubio and Stephany Gregory |  
|=============================|

## Selection Mode:

1. Encryption

2. Decryption

Welcome to the Encryption Machine. Select a mode by inputting a number:

## Encryption Mode (Caesar’s)

Input a string and press ENTER (use only UPPERCASE and SPACE characters):

Input the key and press ENTER:

Your encrypted message is:

## Encryption Mode (Caesar’s)

Input a string and press ENTER (use only UPPERCASE and SPACE characters):

Input the key and press ENTER:

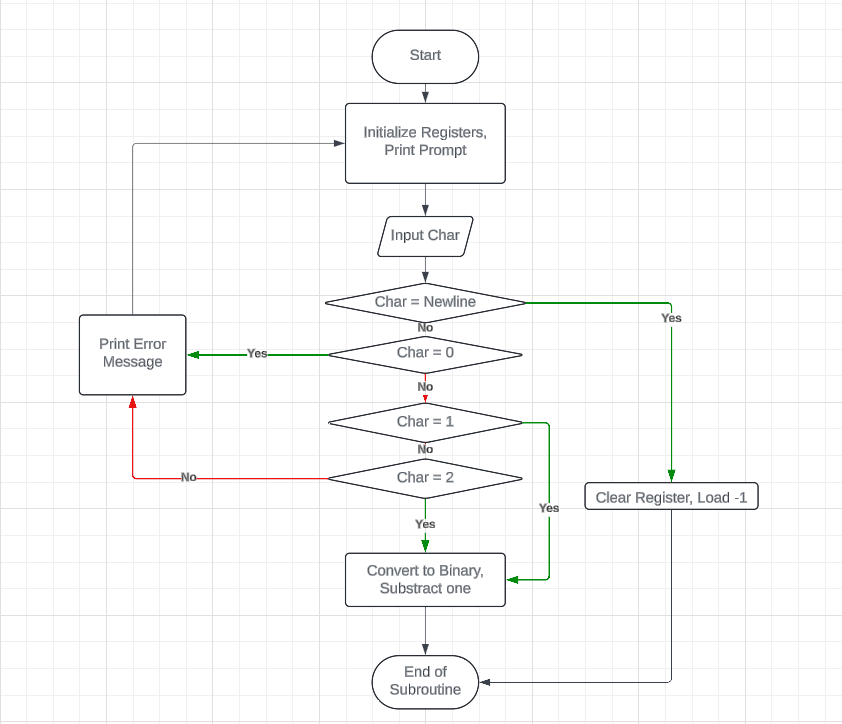
Your decrypted message is:

# Flowcharts

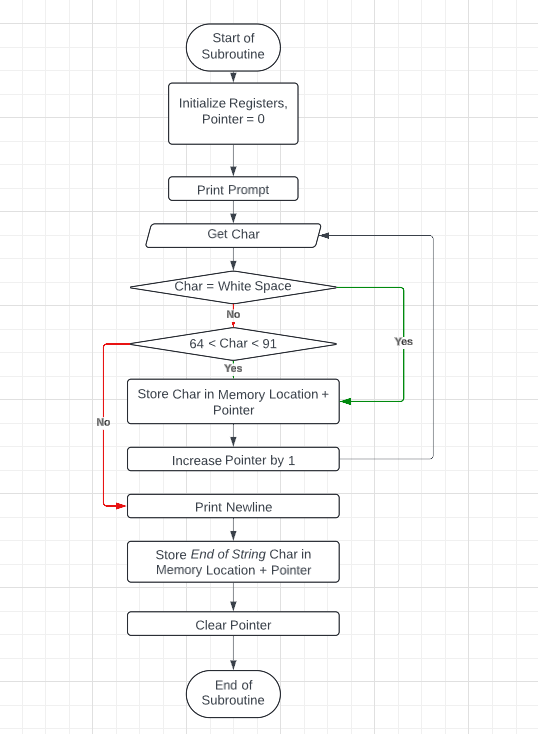
## Main Routine/Program

**(CONTINUES NEXT PAGE)**

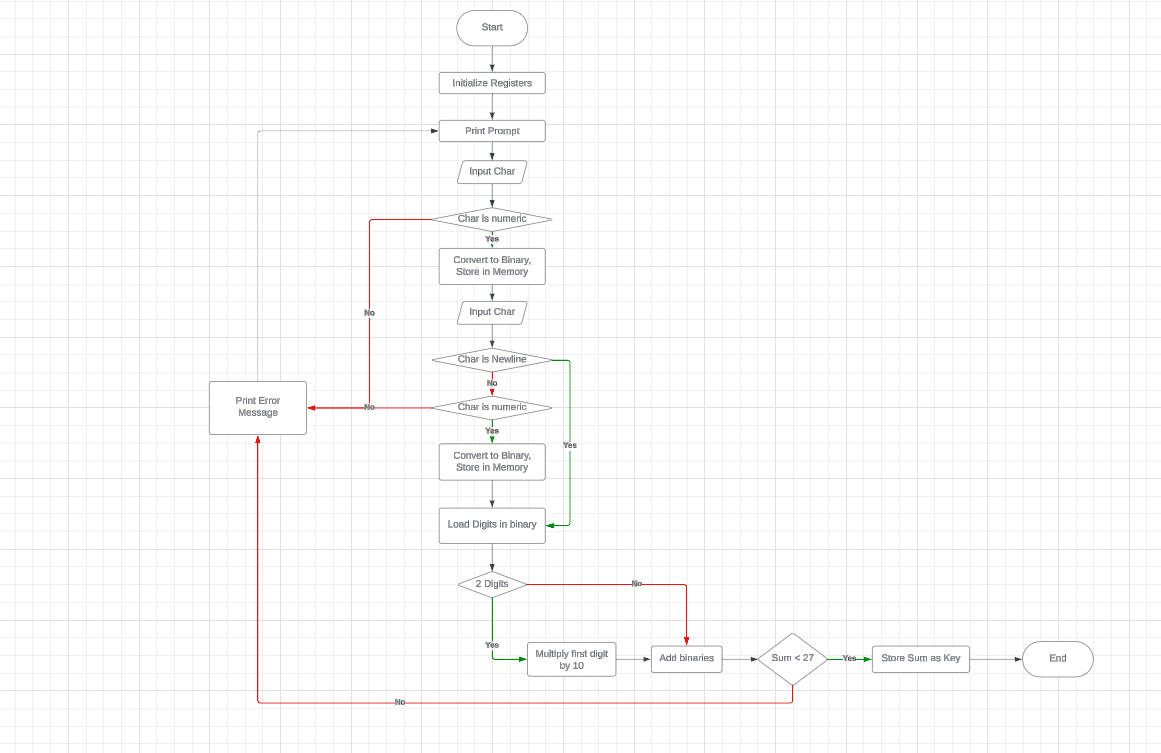
## Selection

**(CONTINUES NEXT PAGE)**

## Input String (Message)

**(CONTINUES NEXT PAGE)**

## Input Key

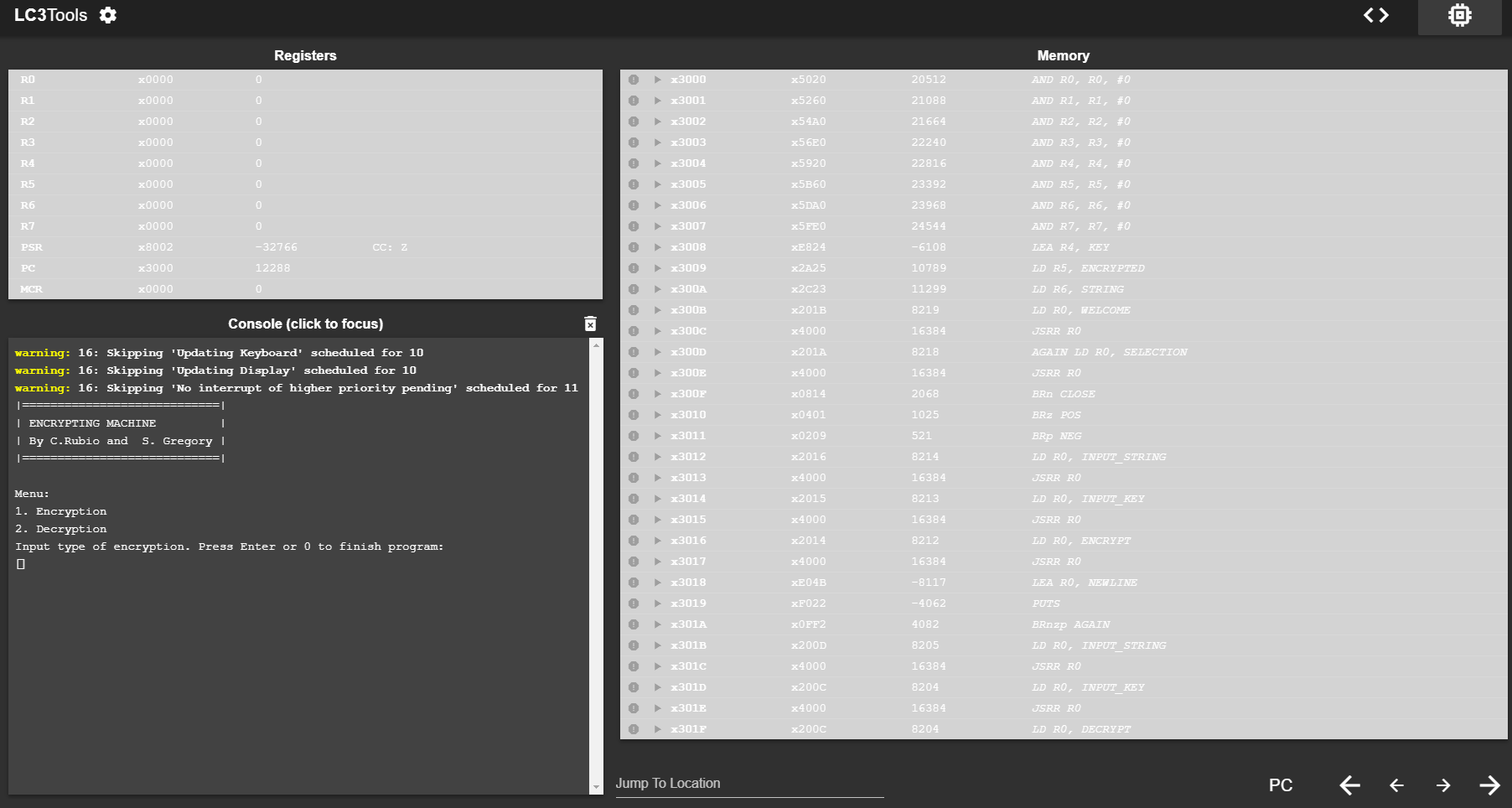
**(CONTINUES NEXT PAGE)**

## Return Encrypted Message



# Screenshots

## Machine Running in LC3

**(CONTINUES NEXT PAGE)**

## Program rejects invalid inputs

## Encryption Mode

## Keys can be of variable number of digits

## Decryption Mode