CSC258 Project[1]

Mar 12 2017

[1] Abdullah Ali and Mohamed Hammoud

This document describes the project proposal for our 258 project.

Our project implements several basic encryption algorithms. The idea is that a user will enter a key to be encrypted, pick the encryption algorithm that they want to use, and once encrypted must enter the code that would result after encryption to unlock it (utilizes ciphers that can be done by hand making this feasible for the user). Once unlocked, an image will display and audio will play signifying a successful unlock.

Milestones

Week 1: Encryption

While the exact encryption algorithm has not been decided on yet, the idea is to use a cipher such as the Caesar Cipher or ROT-13.

The exact implementation of this will require the user to input a code to be encrypted using the keys onboard the DE2 board or perhaps a separate input device. We will then utilize Finite State Machines and shifters as well as registers to read in input and store the encrypted output.

Week 2: Another Encryption Algorithm and the ability to choose

For this milestone, we will implement yet another more complex encryption algorithm. We will also introduce the ability for the user to choose between.

This ability to choose will be done by the user flicking the correct switch on the DE2 board and finite state machines to direct input to the cipher that the user has decided on.

Week 3: Displaying a successful unlock and playing audio

For this milestone, we make it obvious to the user that they have entered the correct code. If the correct code has been entered, an image signifying a successful unlock will appear on screen with celebratory music. If the incorrect code has been entered, an image will be "unsuccessfully decrypted" will appear on a screen and an audible 'failure' sound effect will play.

Project Motivations

What inspired this project was ciphers and encryption algorithms from the past. We found the history of cryptography and the various encryption ciphers used in the past, before modern encryption algorithms as RSA and AES quite fascinating and thought implementing one from a raw hardware perspective would serve as an interesting project and cool 'mechanical' blast to the past.

It relates to the material covered in CSC258 in that almost every major component of the course will be required to get this working properly. We'll require shifterbits and registers to get our actual encryption algorithm working. We'll require finite state machines for user input and outputing an encrypted algorithm. We'll also require memory, the use of a VGA display and an audio component to enable visual confirmation to the user.

This project appeals to me personally because of my fascination with cryptography. The idea of coded messages, having to use basic ingenuity to come up with encryption techniques before the dawn of the computer age strikes me as something quite interesting. To be able to implement this myself using hardware and Verilog (being a Turing complete language) would prove to be an interesting and challenging task.

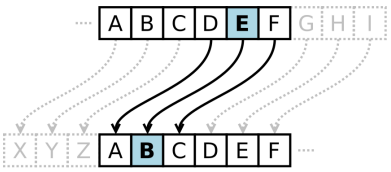

Figure 1: Ex. Caesar Cipher.