Shape

Description automatically generated

**California Polytechnic State University Pomona**

DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING

**Project Report**

Group D

 Alex Beckes, Foad Naeimi, Ignacio Velasco

**Topic**

 Password Protection/Encryption

ECE 3300/3300L

 December 10th, 2023

# Abstract

This project presents the design and implementation of an FPGA-based encryption device that serves as a secure code-activated system, combining elements of password setting, code deciphering, and motor control. The system utilizes a mode selector switch to toggle between password setting and entering modes. In password setting mode, a scrambled number is displayed on the seven-segment display, with the left four segments representing the scrambled code and the right four segments serving as user input. A confirmation color screen is displayed on the VGA screen, guiding the user in whether their guess is correct or incorrect, concurrently using the connected LCD screen allows those with access or authorization to enter the password without all the guesswork or use of cheat sheet. To further enhance security and prevent unauthorized access, a PWM-controlled brushless motor or fan is integrated into the system. The motor or fan serves as a symbolic representation of a critical system, such as a submarine engine. Activation of the motor is contingent upon the correct password entry or successful code deciphering, simulating a security feature vital in situations involving sensitive information, such as nuclear supplies in a submarine.

# Table Of Contents

ABSTRACT…………………………………………………………………………………Page 1

TABLE OF CONTENTS……….…………………………………………………………...Page 2

INTRODUCTION…………………………………………………………………………...Page 3

EXPERIMENTAL SETUP………………………………………………………...Page 3 – Page 4

METHODOLOGY………………………………………………………………...Page 4 – Page 5

RESULTS AND ANALYSIS……………………………………………………...Page 5 – Page 7

CONCLUSION……………………………………………………………………………...Page 8

# Introduction

There are many attempted break-ins from digital to physical sources or even a combination of both, to which the response has been to step up security measures such as password protection, or two-step authentication, or even encryption itself. This project attempts to recreate what steps most companies would theoretically take when it comes to ensuring the security of all important documentation, or components. The inspiration behind the project stems from two dissimilar sources, Cal Poly Pomona’s own method of protection against potential data breaches with two step authentications, and from video games/movies. There is a plethora of spy movies where the secret agent swoops in and easily cracks any codes and steals what is necessary for his mission to be complete. Now all though this is not too far from reality, there is still some sense of questioning when these scenes come up on games or any other forms of media, such as what more could be done to ensure those resources safety/security, and how could we implement something similar in real life. The team set up to build, program, and implement a type of security system that could be theoretically used by government personnel to protect important documentations, such as this project that used an Artix A7 board in order to have one member write a password into the board through the 16 switches available, then use the buttons to load the password into the board and then scramble and change the look and reading of the password, which could serve as a deterrence to any would be thief. The board would be connected via its pmod connectors to an LCD display screen that will save the guess work from the board and just state what the password is. Which would then lead to having the VGA component of the board being connected which prompts the user to input a password, to which the screen would turn blue if correctly entered or red if incorrectly entered, and when entered incorrectly it would trigger a buzzer to serve as an alarm for incorrect password entrance.

# Experimental Setup

The setup of this project relies on the requirements set out by the professor, and some standard equipment when running these kinds of experiments, which required each project to attempt to get these following sections into their projects. The “physical” requirements would be the use or inclusion of a UART, a VGA code and VGA cable, 7-segment display, Switches, and Buttons, all to be used and displayed on a NEXYS A7 Board, with the more digital requirements being a project paper, presentation, and demo. The program(s) used for this experiment were of course VIVADO with two editions for different members due to hardware limitations or requirements.

In order to get started on this project the group first had to determine which kind of project they wished to do for the class. Ultimately Group D decided to implement a kind of encryption tool for their project. The following lists out the various uses for each requirement for the project,

|  |  |
| --- | --- |
| ***Requirement*** | ***Function*** |
| Switches | Serves as the main method of entering a password |
| Buttons | Two buttons are used with the following functions:   |  |  | | --- | --- | | Button one | Load Password | | Button two | System Reset | |
| 7-Segment Display | Split into two sections of four, with the left side representing the numbers to be input as the password, and the right four representing the encrypted and barrel-shifted version of the left four. |
| VGA | The VGA served three purposes, to instruct the user to enter a password, a correct screen, and an incorrect screen. |
| UART |  |

**Figure 1:** Components Used and their functions in the project.

# Methodology

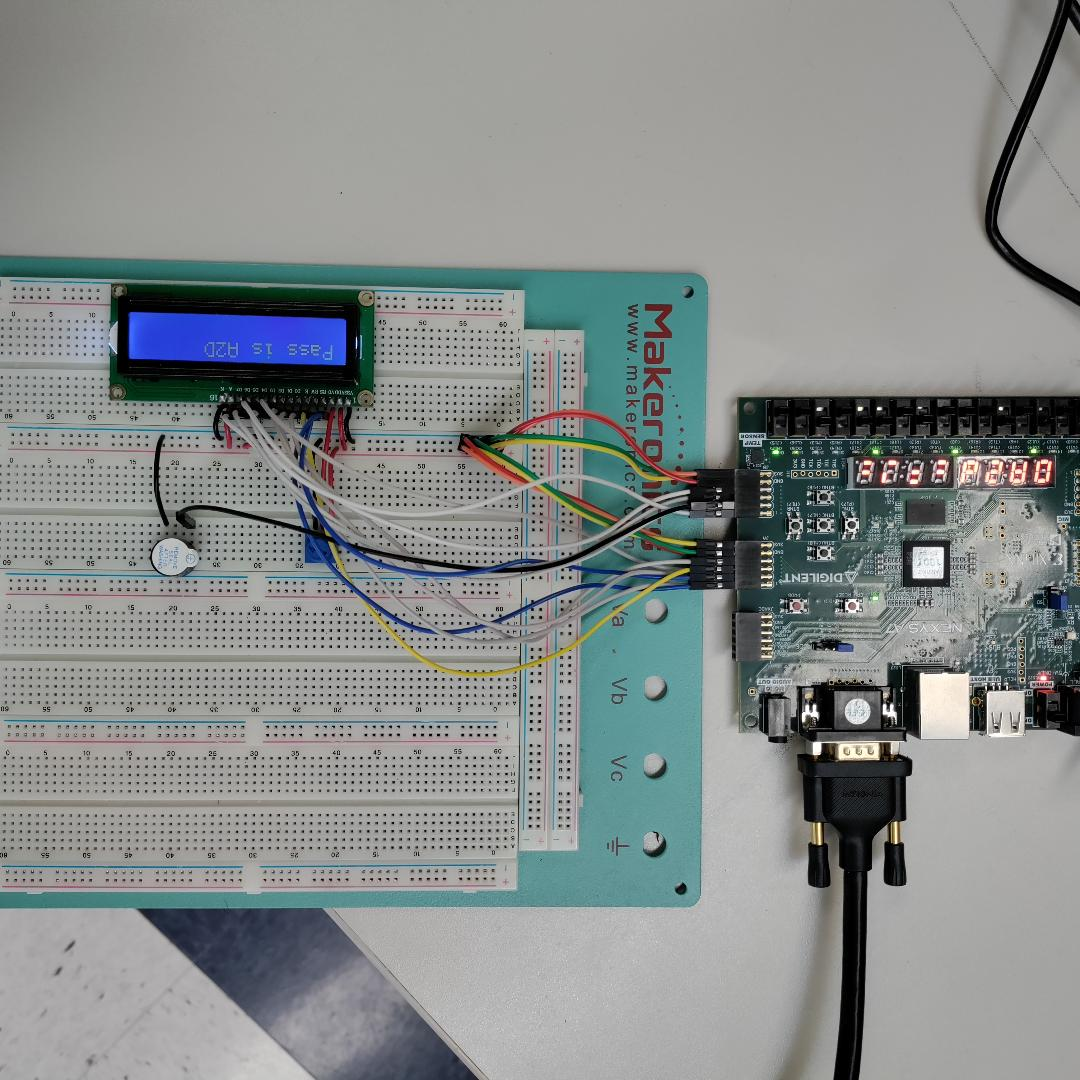
The first step for this project was to develop a basic idea into a working one which was a simple randomizer using a barrel shifter to take a certain string of numbers and mix them up in a certain way which would function as the system’s password set function. Next was developing the method for entering the password, which at this point these first two steps used of a few of the required methods laid out before the group, a button in order to load a password into the system and scramble it with the groups encryption method idea and the 7-segment display. The 7-segment display is sectioned off into two, the first four and the second four which can be seen physically on the board.

A close up of a digital clock

Description automatically generated

**Figure 2:** Sections one and two of the Nexys A7 board.

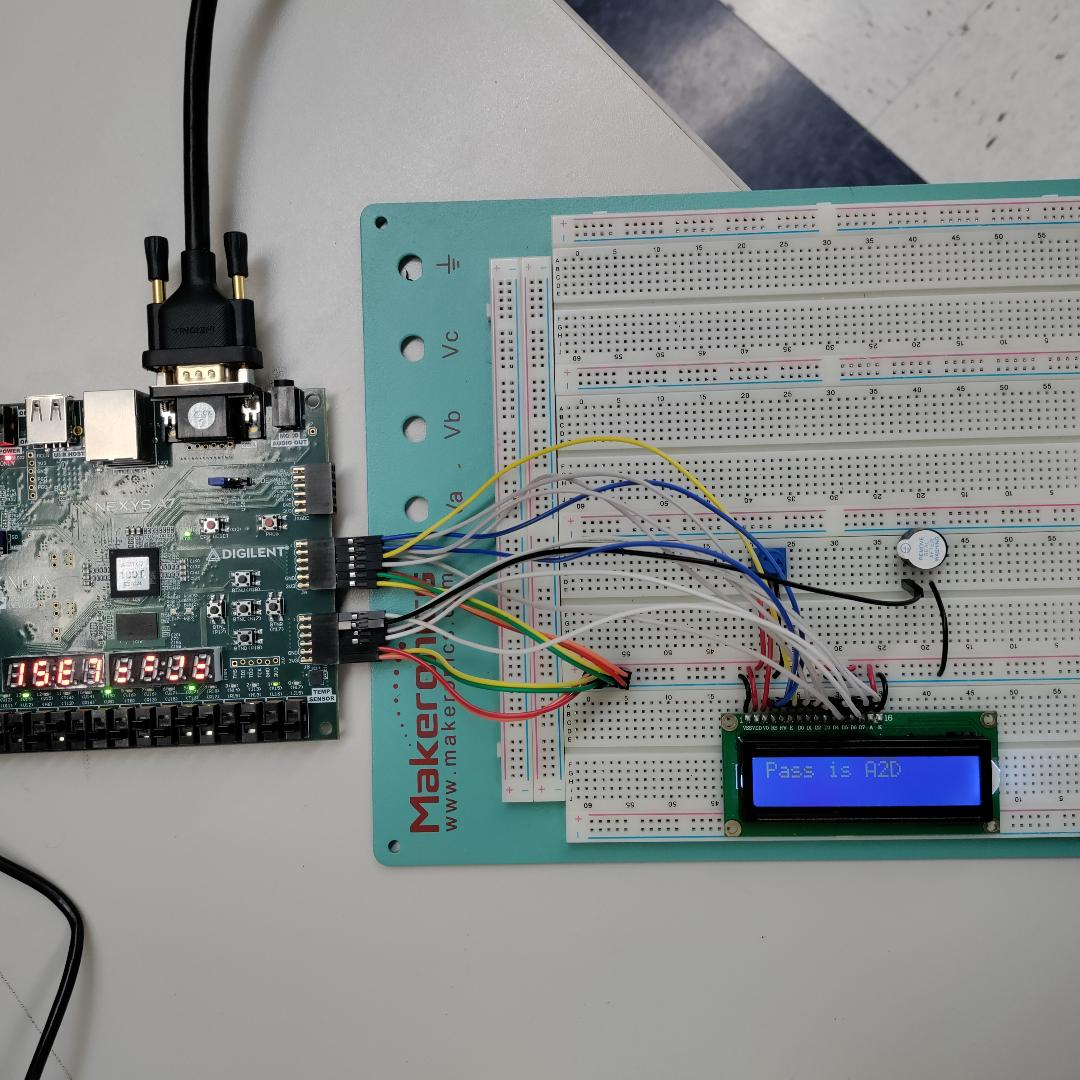
Once in the password entry mode then the switches would be used, in order to input the encrypted password shown on the board, simultaneously the code will be correctly displayed on the LCD screen connected to the boards PMOD, and it will trigger a buzzer to ring, signifying a successful password entry.



**Figure 3:** Nexys A7 board Alongside LCD circuit.

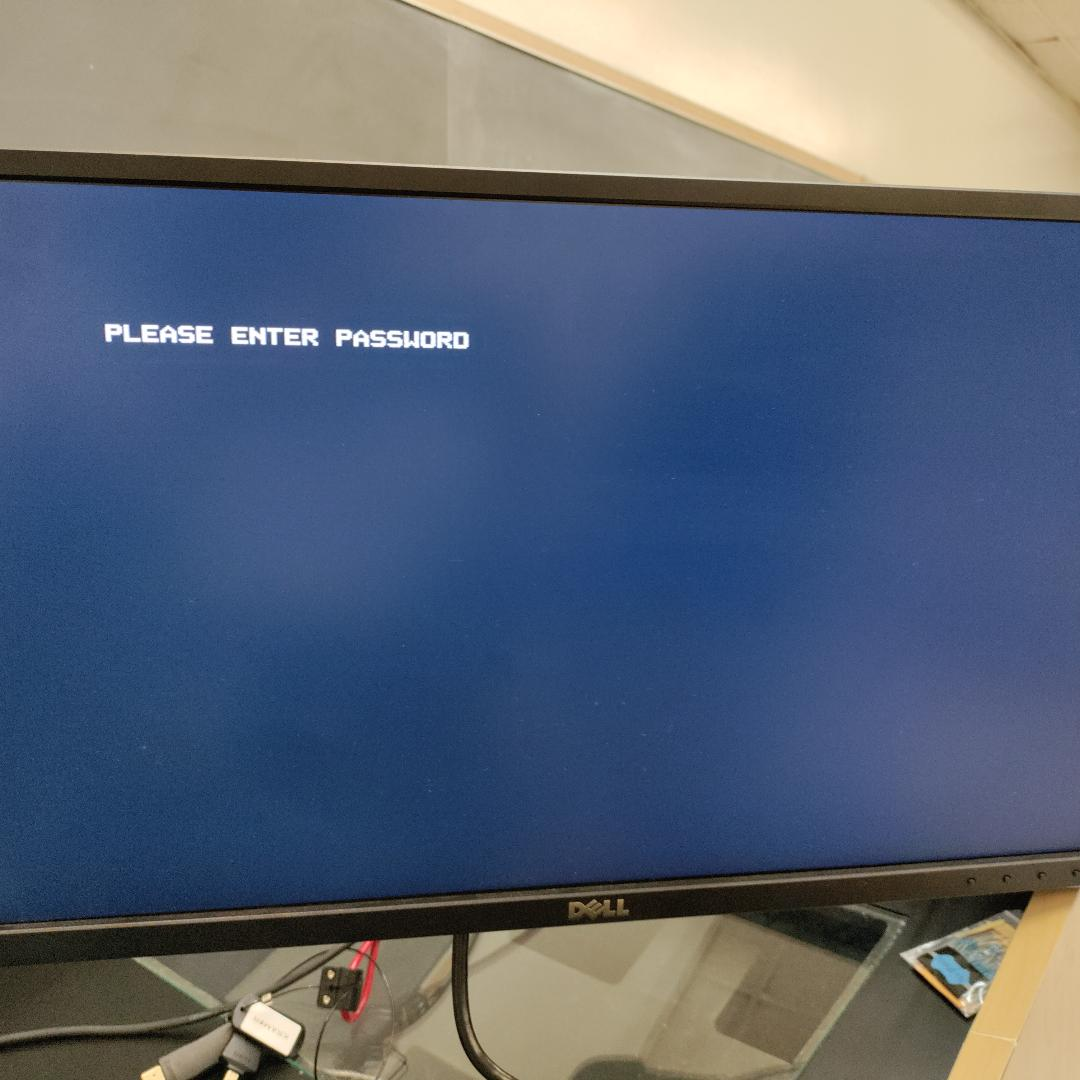
# Results and Analysis

Upon the completion of this project, the team was able to develop all the components and have them working with one another. The first working component was the board itself which housed the encrypted password on “section two” of the board, section two refers to a term coined by the group to denote 7 segment location on board, and “section one” was used as an input display that changed in regard to each switch input on the board. The encrypted password was loaded onto the LCD display in order to allow those authorized easy access to the code and those without left to decipher the code from our own creation. Below are images related to each step with explanations to each picture.



**Figure 4:** Overall Layout of NEXYS A7 along-side LCD circuit.

Figure 3 demonstrates the circuit used for the LCD circuit which connects to two of the PMODS on the board, with it all connecting to a small buzzer that plays a sound when a password is correctly. This then functions in tandem with the VGA since it will display a prompt that instructs the user to please enter a password and will change the screen only once the correct password has been input.



**Figure 5:** VGA output of NEXYS A7 board on screen.

A graph paper with arrows and symbols

Description automatically generated

**Figure 6:** Password Cheat Sheet for Encrypted Password.

# Conclusion

Due to the world’s uncertainty and insecure connections the need for password protection and even encryption is ever present. For this project the group implemented a simple password protected buzzer which sounds mundane, but with everything in the world veering towards smart devices, such as smart TV’s, smart Fridges, and even smart Homes, or even anything that can be broken into by old school brute methods, such as break ins or social engineering for inside threats, one can never be too careful when it comes to potentially hackable objects. There were a few errors that occurred in this project such as the implementation of a green successful login screen displaying once the correct password was entered. With more time the group could have gotten this screen to work, but for now the changing from the login screen to a black screen simulates a successful login from the board.

The group has gained a deeper knowledge and understanding of basic encryption and password implementation on systems, which for this case is the buzzer. This will allow the group to further their own knowledge and alter and improve their code for future uses just for their own knowledge.