DIGITAL PRINCIPLES AND SYSTEM DESIGN PROJECT

Digital code lock system

TEAM MEMBERS:

CSE A , 2nd Year

Jithu Morrison S , 3122 22 5001 051

Ravindran V , 3122 22 5001 701

Jothir Aditya R K , 3122 22 5001 052

Jeevansree E, 3122 22 5001 049

1. Introduction

In response to the escalating demands for heightened security in contemporary access control systems, the Digital Code Lock System has been meticulously designed to be a robust fortress against unauthorized access. This innovative system operates on a foundation of password-based authentication, harnessing the power of advanced combinational logic circuits. Beyond the conventional boundaries of access control, this system grants users the autonomy to set and reset passwords, dynamically adapting to the evolving security landscape.

AIM:

The aim of the "Digital Code Lock System" project is to create a strong and easy-to-use access control system. Imagine a high-tech lock for a room or building. This system ensures that only authorized people can enter while providing a straightforward experience for users.

COMPONENTS REQUIRED:

S.NO	COMPONENTS REQUIRED	SPECIFICATIO N	QUANTITY
1.	T Flip-Flop	IC 7473	8
2.	D Flip-Flop	IC 7474	3
3.	LED (Light Emitting Diode)	-	4
4.	2x1 Multiplexer	IC 74157	3
5.	1x2 Demultiplexer	IC 74139	3
6.	2 Bit up counter	IC 74161	2

7.	**Debounce buttons**	**-**	**2**
8.	**NOT Gate**	**IC 7404**	**14**
9.	**AND Gate**	**IC 7408**	**24**
10.	**OR Gate**	**IC 7432**	**4**
11.	**XOR Gate**	**IC 7486**	**8**
12.	**4x2 Priority Encoder**	**IC 74147**	**1**
13.	**Bread Board**	**-**	**3**
14.	**Connecting Wires**	**-**	**As required**
15	**16 bit LED Display**		**9**

Scope:

The "Digital Code Lock System" project aims to develop a strong and user-friendly access control solution using advanced combinational logic circuits and digital principles. Focused on password-based authentication, the system empowers users to set and reset passwords through a secure interface. Key features include intricate password verification, secure storage using encryption, and protection against unauthorized access attempts. The system architecture incorporates various components like Flip-Flops, LEDs, Multiplexers, Demultiplexers, and Logic Gates. Implementation details ensure secure password storage and user-centric design. Future enhancements include exploring biometric authentication, additional security layers, and the potential for remote management capabilities. The project aims to provide a reliable, adaptable, and innovative solution for access control, addressing current security needs and allowing for future flexibility.

2. System Features

2.1 Password Verification

The linchpin of the Digital Code Lock System is its prowess in password verification. Through the intricate orchestration of combinational logic circuits, the system meticulously scrutinizes user-entered passwords against pre-set codes. This process transcends mere matching; it demands a pixel-perfect alignment between the entered code and the stored password, creating an impregnable barrier against unauthorized entry attempts.

2.2 Password Setting

User empowerment takes center stage with the Password Setting feature. Beyond the perfunctory act of selecting a password, users are guided through a designated interface that not only ensures a seamless experience but enforces stringent security requirements. The chosen passwords are stored with the utmost security, establishing the bedrock for a reliable and fortified access control mechanism.

2.3 Password Resetting

The system's adaptability shines in the Password Resetting feature. For users grappling with forgotten passwords or those seeking a periodic change, the system unveils a secure password-resetting process. This user-guided journey prioritizes security, steering clear of compromise while facilitating a streamlined means for users to regain access without undue complexity.

3. System Design

3.1 Architecture

At the core of the Digital Code Lock System is a meticulously crafted combinational logic design. This architectural choice ensures that the system's output is intricately tied to the current input, resulting in a deterministic and predictable behavior crucial for robust access control. Logic gates and a constellation of combinational components work harmoniously, creating an efficient framework for processing and comparing password data.

3.2 Components

Password Storage: Encryption techniques form the bulwark of password storage, safeguarding passwords against prying eyes. Robust algorithms fortify the system against insidious threats such as brute-force attacks, ensuring the sanctity of stored passwords.

Combinational Logic Circuit: This critical component of the system undertakes a digit-by-digit comparison between the entered and stored passwords. The meticulous nature of this process ensures that access is a privilege earned only when all digits align perfectly, thwarting any attempts at unauthorized access.

Output: The Output Interface is not merely a notifier of access status; it is a conduit of clarity. It communicates, in unequivocal terms, whether access is granted or denied, thereby empowering users with immediate and comprehensible feedback.

4. Implementation Details

4.1 Password Storage

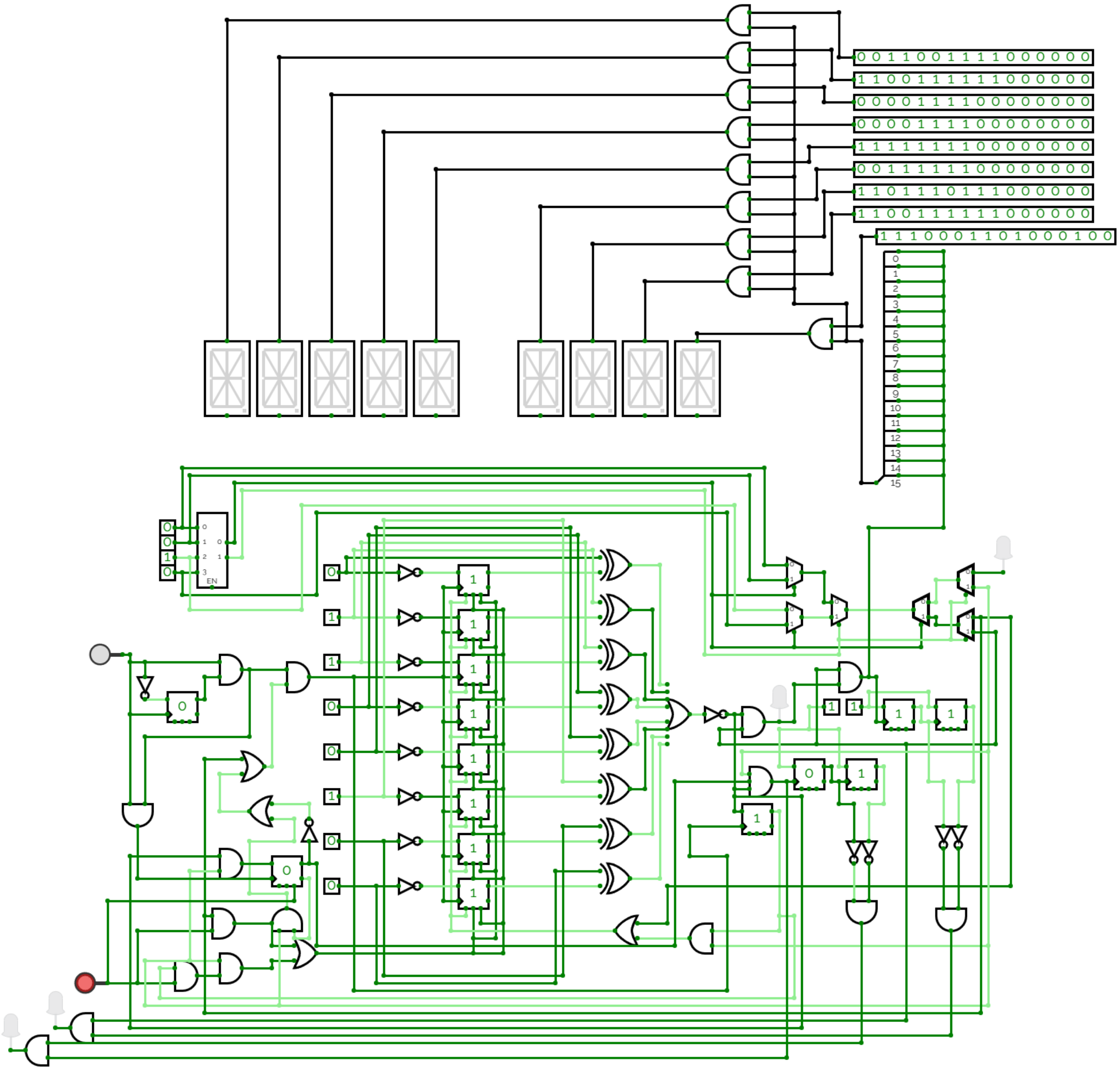
The fortification of the system begins with the implementation of secure password storage. Encryption techniques, ranging from industry-standard to cutting-edge, are employed to shield passwords from potential breaches. These cryptographic safeguards, coupled with robust algorithms, erect an impervious barrier against unauthorized access attempts, including the persistent threat of brute-force attacks.

4.2 Combinational Logic Circuit

The essence of password verification lies in the Combinational Logic Circuit. This intricate circuitry navigates through each digit of the user-entered password, engaging in a nuanced dance of comparison with the corresponding digits of the stored password. Access, the ultimate outcome, is a binary decision—granted only when every digit aligns perfectly, and denied in all other instances.

PROCEDURE AND METHODOLOGY:

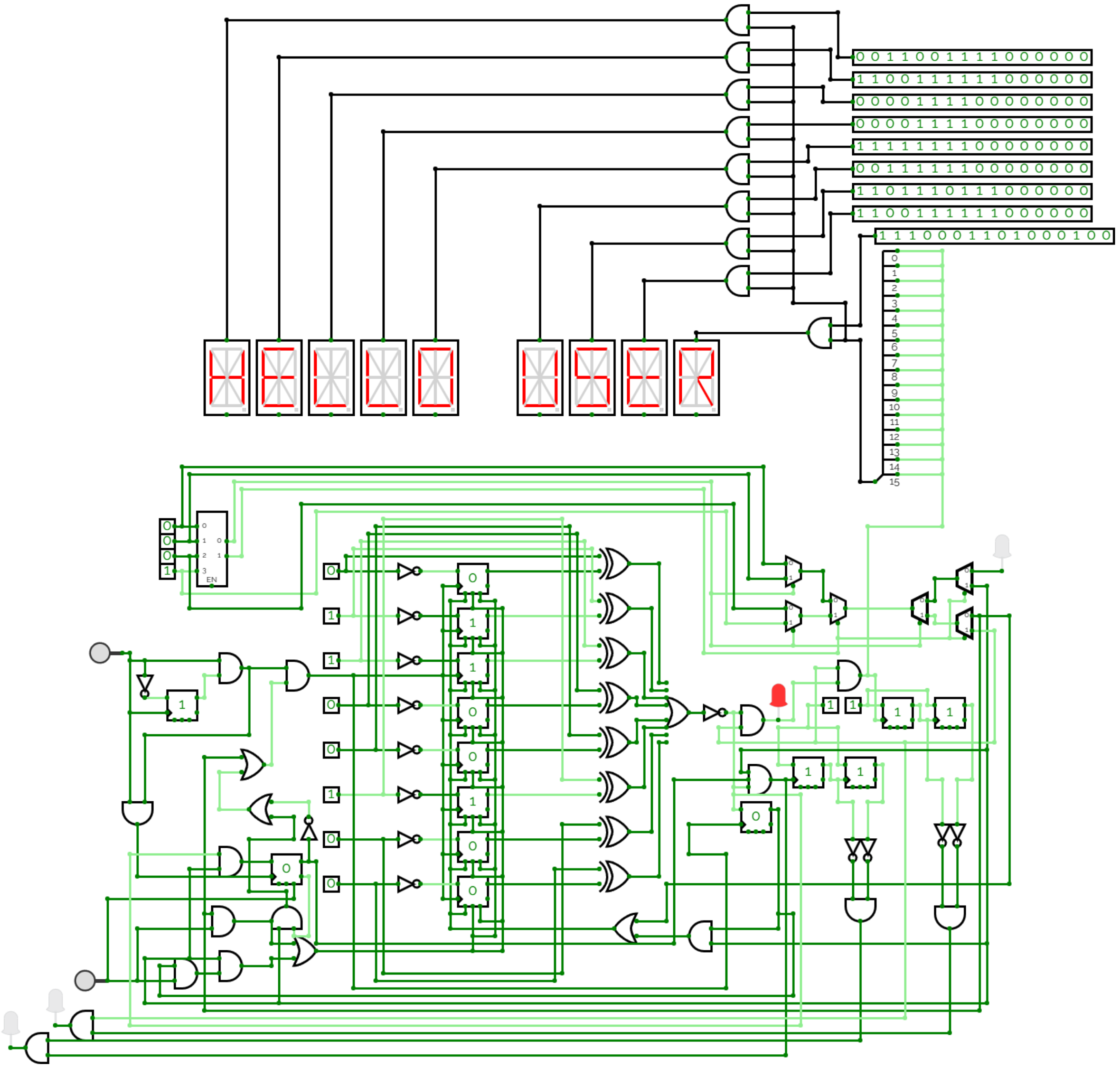
The procedure and methodology for building a Digital code lock system involves several key steps and components. Here we can set, reset or verify passwords. This system has 3 core parts: the first one is setting the password, where if we forgot the password, we can set a new password by refreshing the system and setting a new password and the second one is too reset the password you can only reset the password if you know the previous password, where you need to verify password too conform its the previous password and set a new password, and also the third option is to verify password so that we can open what we need.



STEP-1: Setting password: The foundational step in configuring the Digital Code Lock System involves the seamless establishment of a user-defined password. Through an intuitive and user-friendly interface, users can effortlessly set and create unique passwords, fostering a sense of ownership and customization in their security experience. The secure storage of these passwords forms the bedrock of the system, with encryption techniques employed to shield them from potential breaches. The password can be set by refreshing the system so there won't be some junk values then we can set the password and store it using a debounce button.

<u>STEP-1: Resetting password: </u>Resetting passwords can be done if and only if the previous password is known. So first the password needs to be verified and then we can change the password by refreshing and then setting a new password and there is a system that indicates when password is changed more than 3 times.

<u>STEP-1: Verify password:</u>



Passwords can be verified by entering a password. If the entered password is the same as the stored password, a light glows and text "HELLO USER" is displayed. If a password is entered 3 times a light glows.

Components used:

1. Button0 and Button1:

- These modules simulate buttons, and their outputs toggle on each positive edge of an associated signal (some_signal for Button0 and some_other_signal for Button1).

2. D FlipFlop:

- This module represents a D flip-flop, a basic memory element. It stores the input (`d`) on the rising edge of the clock (`clk`).

Truth Table:

Q(t)	D	Q(t+1)
0	0	0
0	1	1
1	0	0
1	1	1

(X means don't care)

3. T FlipFlop:

- This module represents a T flip-flop. It toggles its state (`q`) on each rising edge of the clock (`clk`) when the input T (`t`) is 1.

Truth Table:

T	Q(t)	Q(t+1)
0	0	0
0	1	1
1	0	1
1	1	0

(X means don't care)

4. Multiplexer 2X1**:**

- This module is a 2-to-1 multiplexer. It selects either `in0` or `in1` based on the value of `sel`.

Truth Table:

A	B	S0	Y
A	0	0	A
0	A	1	A

(X means don't care)

5. Demultiplexer 1X2**:**

- This module is a 1-to-2 demultiplexer. It distributes the input `in` to either `out0` or `out1` based on the value of `sel`.

Truth Table:

A	S0	Y1	Y2
A	0	A	0
A	1	0	A

(X means don't care)

6. PriorityEncoder 4x2:

- This module is a 4-to-2 priority encoder. It encodes the highest-order active input to a 2-bit binary code.

Truth Table:

I3	I2	I1	I0	Y1	Y0
0	0	0	0	X	X
0	0	0	1	0	0
0	0	1	X	0	1
0	1	X	X	1	0
1	X	X	X	1	1

(X means don't care)

5. Conclusion

The Digital Code Lock System isn't merely a gatekeeper; it's an embodiment of reliability and security in the realm of access control. The symbiotic fusion of combinational logic for password verification and user-centric features like password setting and resetting establishes it as a versatile, user-friendly, and indispensable solution applicable across diverse domains.

6. Future Enhancements

The forward trajectory of the Digital Code Lock System beckons towards innovations that transcend contemporary norms. The integration of biometric authentication emerges as a tantalizing prospect, enhancing the multifactorial nature of security. Additional security layers, fortified against emerging threats, could be seamlessly woven into the system's fabric. Remote management capabilities stand as a beacon on the horizon, promising a future where the system's efficacy extends beyond the confines of physical proximity.