DEPARTMENT OF ELECTRONICS
AND COMMUNICATIONS
ENGINEERING
VELLORE INSTITUTE OF
TECHNOLOGYCHENNAI – 600 127

DIGITAL SYSTEMS DESIGN
BECE102L

SEQUENTIAL PASSWORD PROTECTOR

Jayanth.S.B 22BEC1053
Himesh Potnuru 22BEC1004

Acknowledgement

We wish to express our sincere thanks and a deep sense of gratitude to our project guide, B. Lakshmi, School of Electronics Engineering, for her consistent encouragement and valuable guidance offered to us in a pleasant manner throughout the course of the project work. We are extremely grateful to Dr. Susan Elias, Dean of the School of Electronics Engineering, VIT Chennai, for extending the facilities of the school towards our project and for her support. We express our thanks to our Head of the ECE Department Dr. Mohanaprasad K. for his support throughout the course of this project. We also take this opportunity to thank all the faculty of the school for their support and their wisdom imparted to us throughout the course. We thank our parents, family, and friends for bearing with us throughout the course of our project and for the opportunity they provided us in undergoing this course in such a prestigious institution.

Abstract

The 'Sequential Password Protector' project fortifies digital system security using 8-bit character passwords and essential digital logic components like logic gates, multiplexers, encoders, decoders, flip-flops, and adders. Focused on enhancing access control, the project embeds a predetermined 8-bit character sequence within the circuitry, mandating a precise binary input for access. It relies on multiple individual digital IC chips significantly enhancing security. This project underscores the pivotal role of digital logic in safeguarding systems. It lays the foundation for advanced security applications across diverse domains. With potential applications in computer security, physical access control, industrial systems, encryption key management, and document security, its adaptability underscores its potential to elevate security measures significantly. The functional 'Sequential Password Protector' serves as a robust security solution, driving advancements in digital system security.

Index

Introduction

The "Sequential Password Protector " aims to bolster digital system security through the application of fundamental digital logic principles. By employing 8-bit character passwords and utilizing logic gates, Multiplexers, Encoders, Decoders, Demultiplexers, Flipflops and Adders, this project establishes a robust password protection mechanism. Users must input the correct binary sequence to gain access, offering a considerable degree of security. It proposes an alternative to magnitude comparators digital locks. The circuitry utilizes a plethora of digital IC chips instead of a microcontroller which can potentially be hacked giving such locking systems a decisive advantage. The password is preset and contained in the circuitry making it extremely difficult to bypass the system.

This endeavor underscores the importance of comprehending digital logic's role in safeguarding digital systems. While it provides a rudimentary solution, it serves as a stepping-stone for more advanced security implementations.

By blending theoretical foundations with practical application, this project contributes significantly to the domain of digital system security, paving the way for future advancements in the field. It has a wide array of applications in a variety of fields including but not limited to

1. **Computer and Network Security:** The device can be used as an additional layer of security in computer systems and networks. Users would need to input the correct 8-bit character password sequence to gain access to sensitive data, applications, or network resources. This can help protect against unauthorized access and data breaches.

2. **Physical Access Control:** Beyond digital systems, the device could be adapted for physical access control, such

as securing doors, safes, or restricted areas. Users would need to enter the correct sequence to unlock doors or access specific physical locations, enhancing security in buildings or facilities.

3. **Industrial Control Systems:** In industrial settings, the device can be employed to control access to critical machinery, equipment, or control systems. By requiring the correct 8-bit character password sequence, it can prevent unauthorized personnel from tampering with industrial processes, ensuring safety and operational integrity.

4. **Data Encryption Key Management:** The device can serve as a part of a multi-factor authentication system for accessing encrypted data. Users would need to provide the correct password sequence as one of the authentication factors before gaining access to sensitive information. This can be particularly valuable in securing confidential data in storage or during transmission.

5. **Secure Document Storage:** It can be used in applications where secure document storage is crucial, such as government agencies, financial institutions, or legal firms. The device could be integrated into secure file cabinets or storage units, ensuring that only authorized individuals can access sensitive documents.

Components

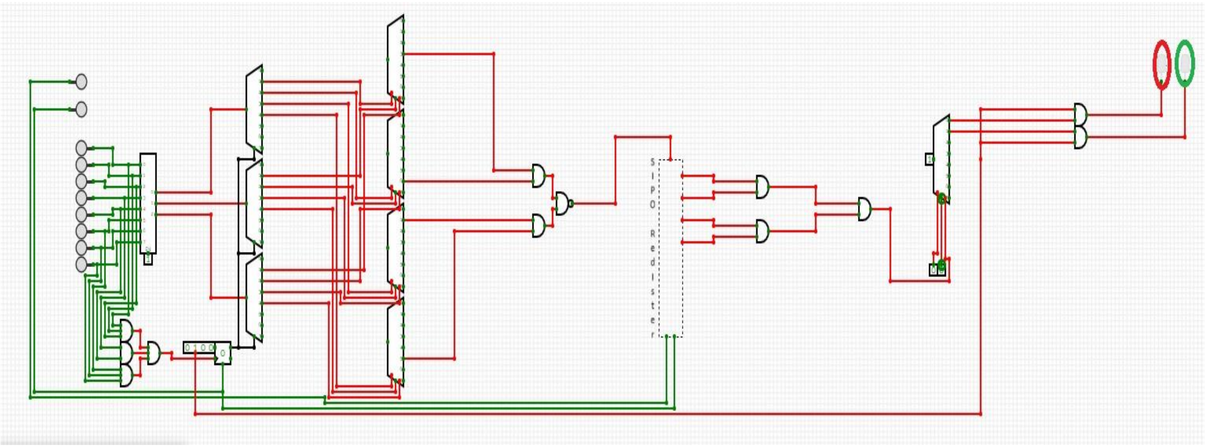
- Single Core Breadboard Jumper Hookup Wire
- Wire Cutter
- Breadboards
- Push Buttons
- (1:8 Demultiplexer) IC74138
- (4-Bit Binary Counter) IC74193
- (Serial-In-Parallel-Out Shift Register) IC74164
- (8:3 Priority Encoder) IC74148
- (2-Input AND Gate) IC7408
- (3-Input AND Gate) IC7411
- (2-Input OR Gate) IC7432
- (3-Input OR Gate) IC4075
- Red LED
- Green LED
- Resistors
- (D-Flipflop) IC7474
- 5V (Battery) Voltage Source
- (9V-5V Voltage Regulator) IC7805
- (2-Input NOT Gate) IC7404

Methodology

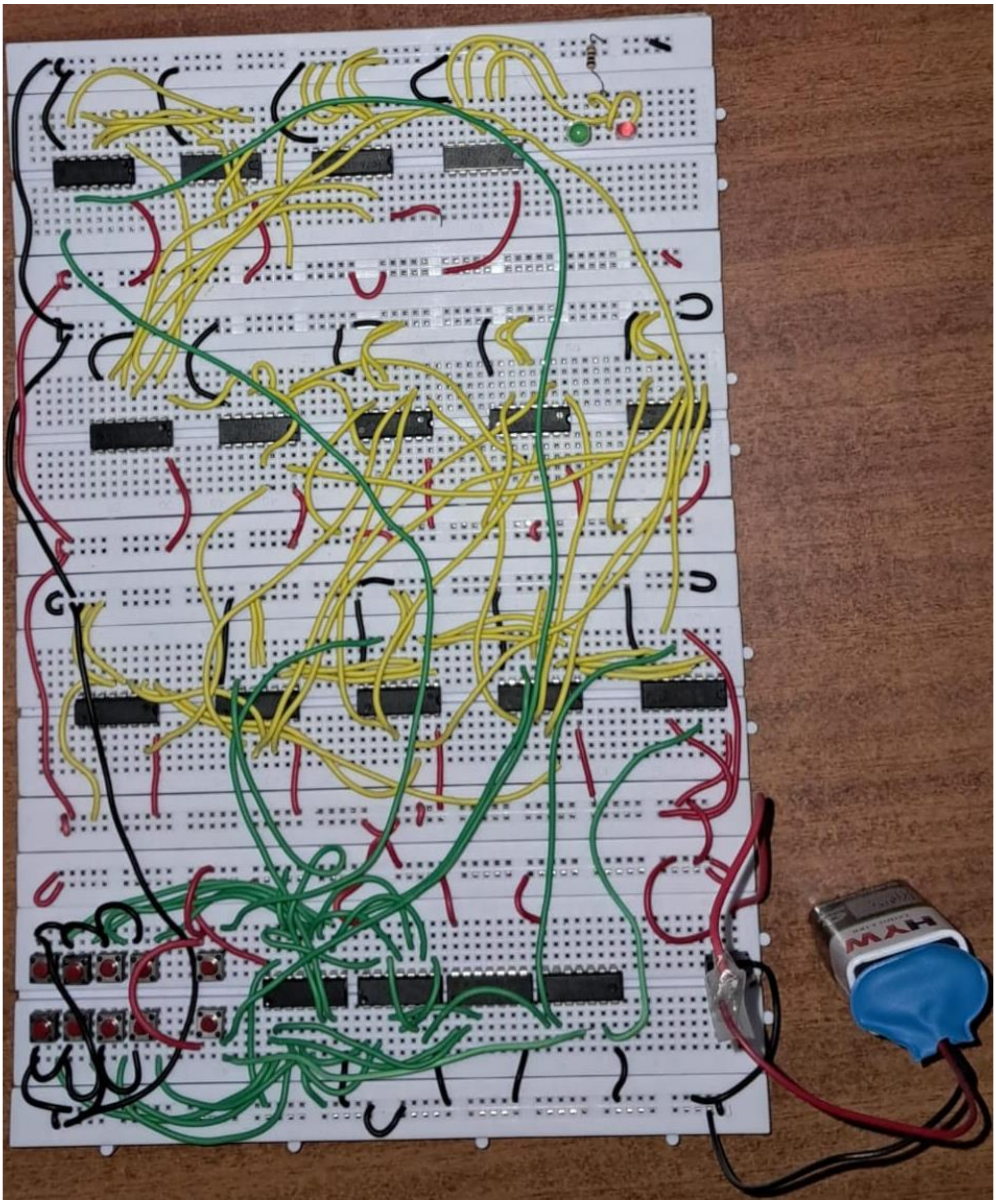
The circuit is a password protector that unlocks when the right sequence is entered. Push button switches (1-8) are utilized to take input from users. The user must enter an 8-bit sequence predetermined and embedded into the circuit correctly to activate the green LED; else the red LED is activated. There is also a reset button that is used to reboot the circuit.

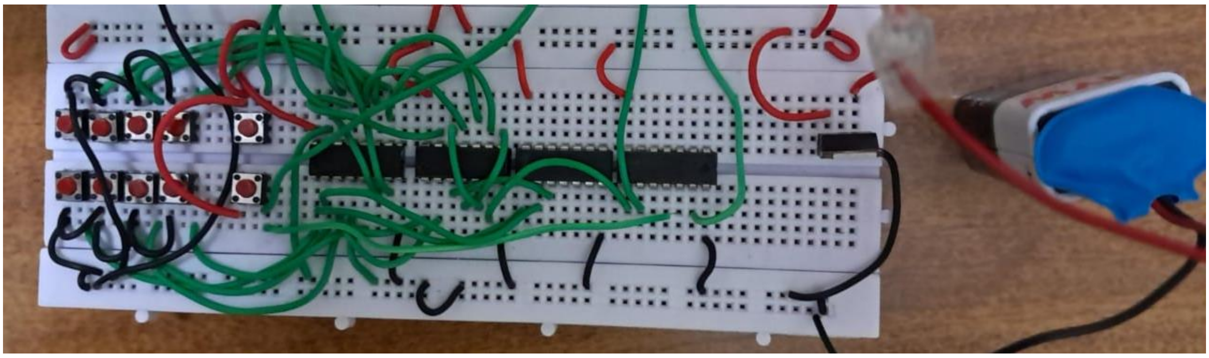
The input from the push button switches is transmitted to an 8-bit priority encoder which maintains a default high. The buttons are also sent to a series of and gates and subsequently to a 4-bit binary counter. The encoder sends 3 bits of encoded input data to the inputs of 3 8-bit demultiplexers. The 3 selection lines of each demultiplexer stem from the first 3 output lines of the counter in parallel. The first demultiplexer provides s0 LSB selection line for 8 demultiplexers in the next stage of the circuit. Similarly, the second demultiplexer outputs are sent to s1 selection lines of 4 different demultiplexers and third demultiplexer outputs are sent to s2 selection lines for the next stage. These 8 demultiplexers have default input 0 and only 1 proceeding output line. The output lines selected in these multiplexers determine the password values and sequence of the circuit. These predetermined output lines are sent to a series of and gates. The emerging output line is sent to a series-in-parallel-out 8-bit shift register. The output lines of the shift register are connected to or gates and added meaning all of them must be high to give output 1. The emerging output is sent to the s0 selection line of an 8-bit demux with input high and s1 and s2 selection lines on low. The y0 output is connected to a red LED and y1 is connected to a green LED. The reset switch is connected to both the counter and the shift register.

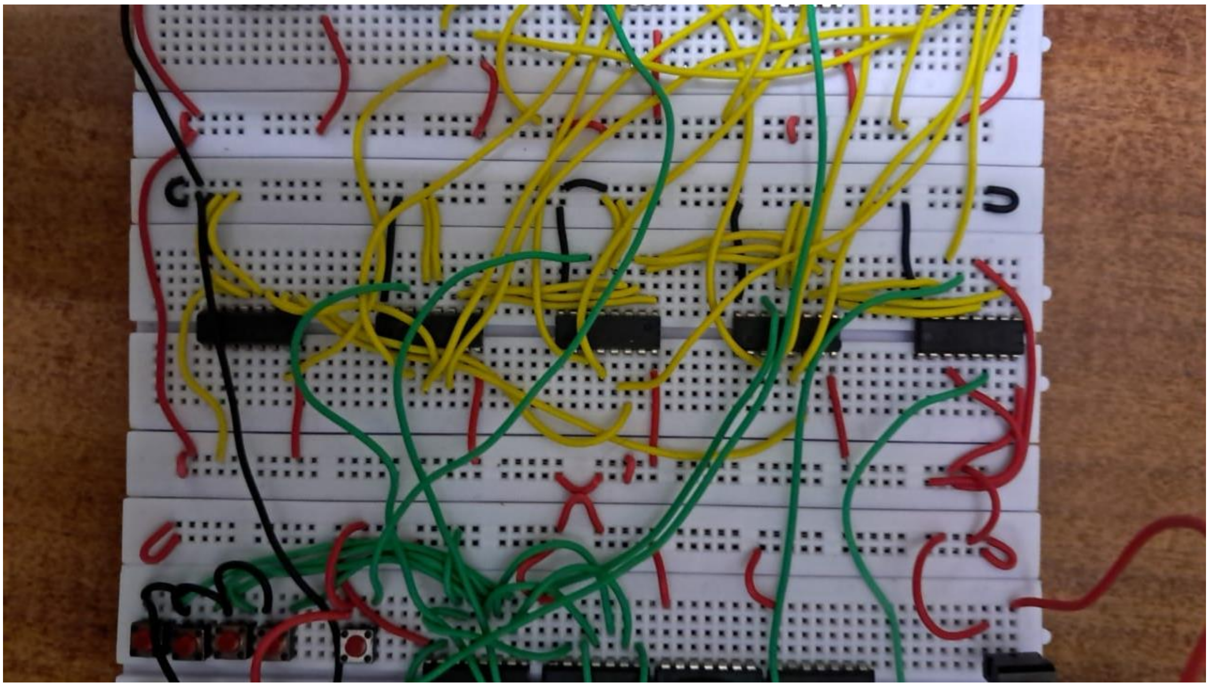
Circuit Diagram

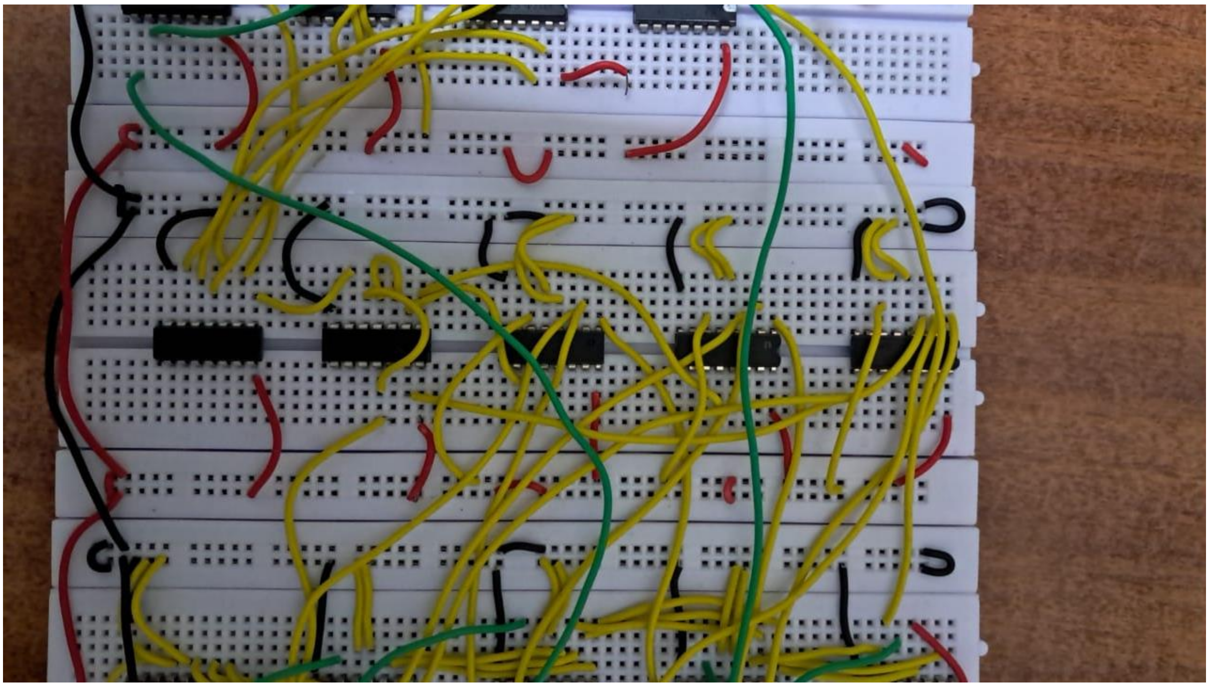


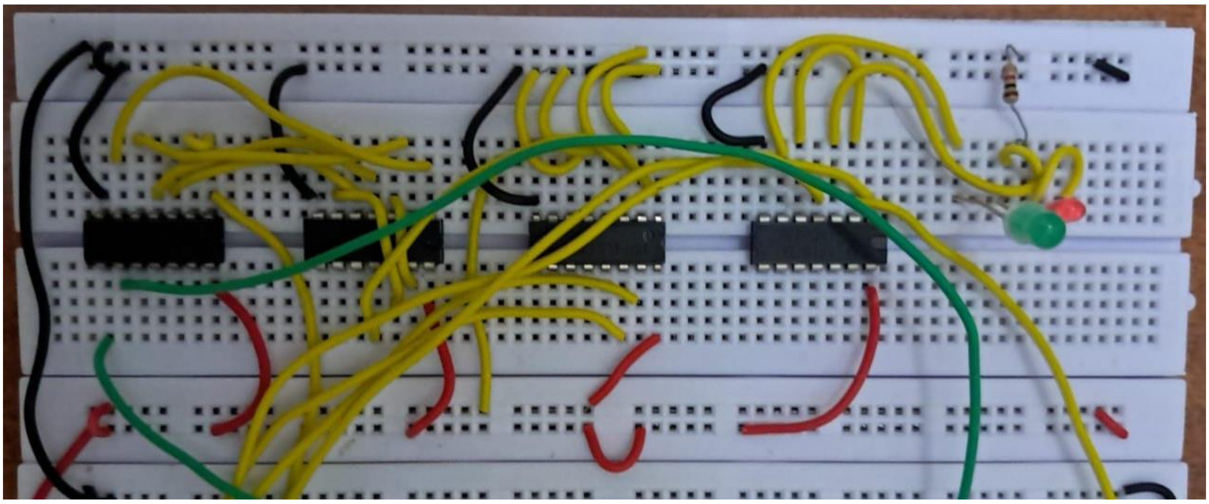
Result











DEMONSTRATION:<https://youtu.be/Y7aCvkQvEQo?si=9Ahc1w--HeAo26rg>

Conclusion

To summarize, the 'Sequential Password Protector' project demonstrates a robust security mechanism achieved through the amalgamation of fundamental digital logic components. This innovative system employs 8-bit character passwords and a network of logic gates, multiplexers, encoders, decoders, flip-flops, and adders to fortify access control.

The primary objective of this project is to fortify security in digital and physical access scenarios. Utilizing a predetermined 8-bit character sequence embedded within the circuitry, the system mandates the accurate input of a binary sequence for access. This approach offers a significant level of security, distinguishing itself from vulnerable microcontroller-dependent digital locks by leveraging numerous digital IC chips for heightened security.

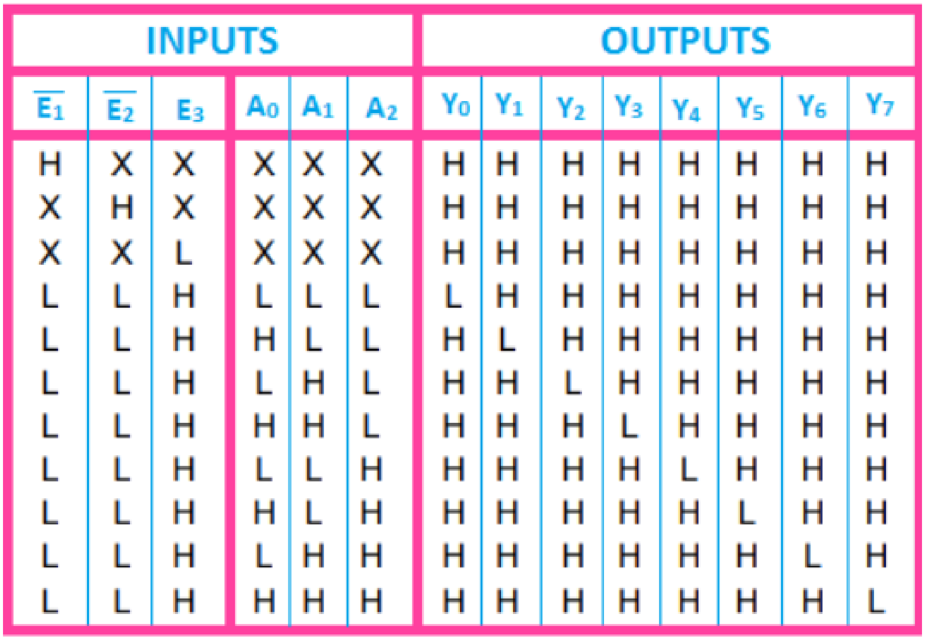
By merging theoretical underpinnings with practical application, this project highlights the pivotal role of digital logic in safeguarding systems. While serving as an initial solution, it lays the groundwork for more advanced security implementations across diverse domains.

Moreover, the project's adaptability is notable, with potential applications in computer and network security, physical access control, industrial systems, data encryption key management, and secure document storage. Its flexibility across multiple sectors underscores its capacity to elevate security measures significantly.

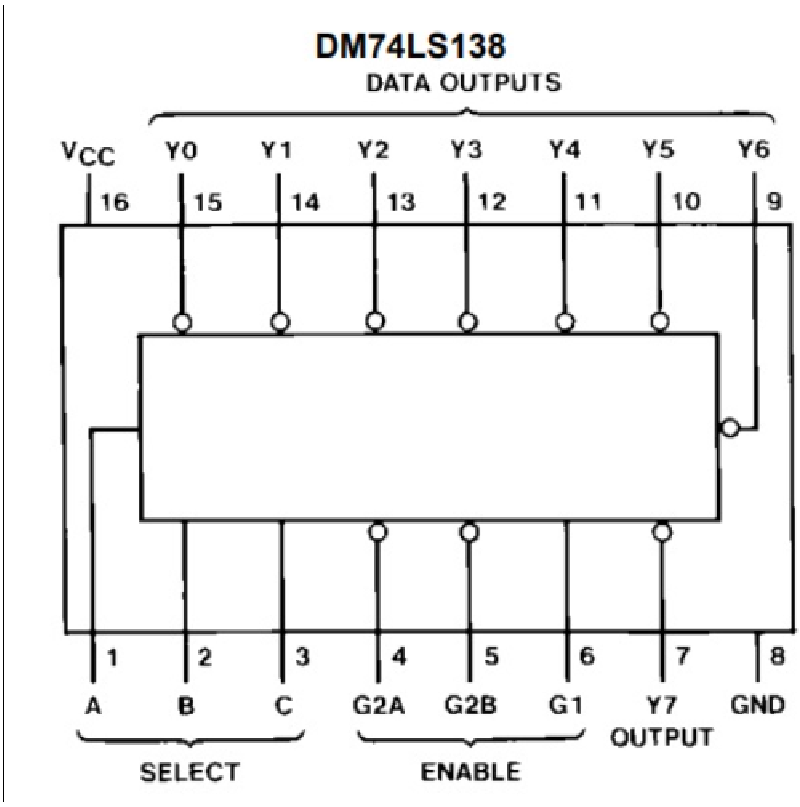
The successful implementation and operational demonstration of the 'Sequential Password Protector' underscores its efficiency as a robust security solution, setting the stage for future advancements in digital system security.

Data Sheets

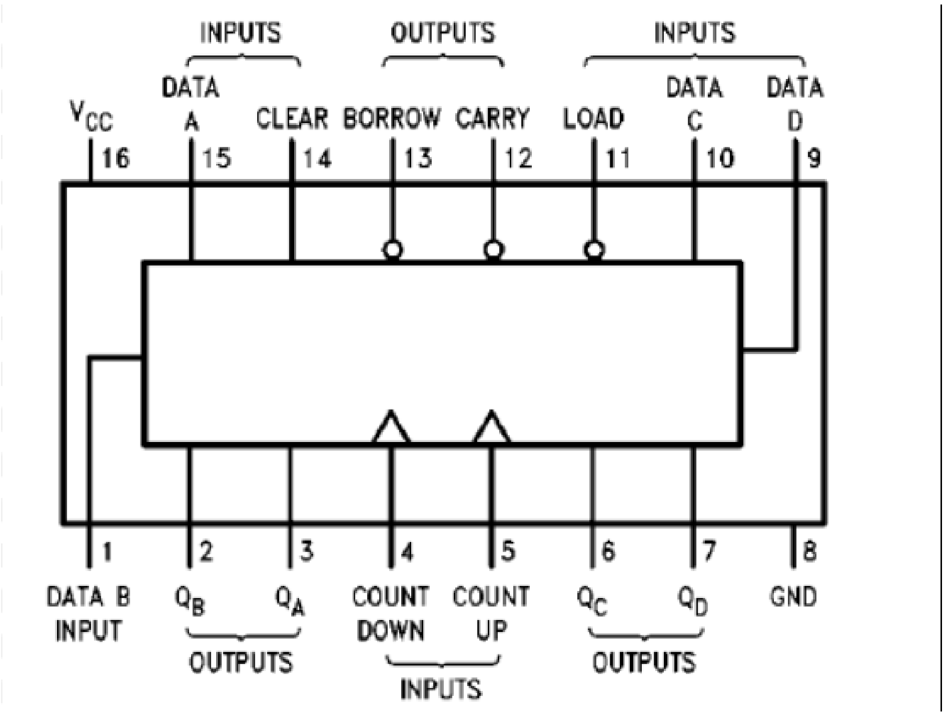
IC74138

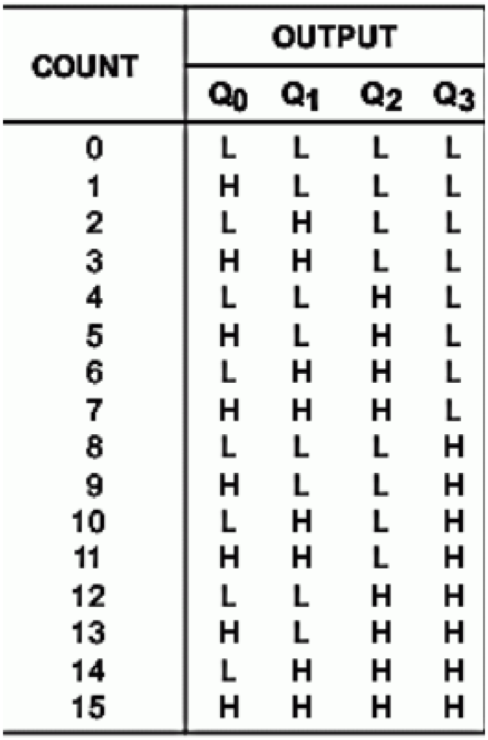


INPUTS						OUTPUTS							
$\overline{E_1}$	$\overline{E_2}$	E_3	A_0	A_1	A_2	Y_0	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7
H	X	X	X	X	X	H	H	H	H	H	H	H	H
X	H	X	X	X	X	H	H	H	H	H	H	H	H
X	X	L	X	X	X	H	H	H	H	H	H	H	H
L	L	H	L	L	L	L	H	H	H	H	H	H	H
L	L	H	H	L	L	H	L	H	H	H	H	H	H
L	L	H	L	H	L	H	H	L	H	H	H	H	H
L	L	H	H	H	L	H	H	H	L	H	H	H	H
L	L	H	L	L	H	H	H	H	H	L	H	H	H
L	L	H	H	L	H	H	H	H	H	H	L	H	H
L	L	H	L	H	H	H	H	H	H	H	H	L	H
L	L	H	H	H	H	H	H	H	H	H	H	H	L



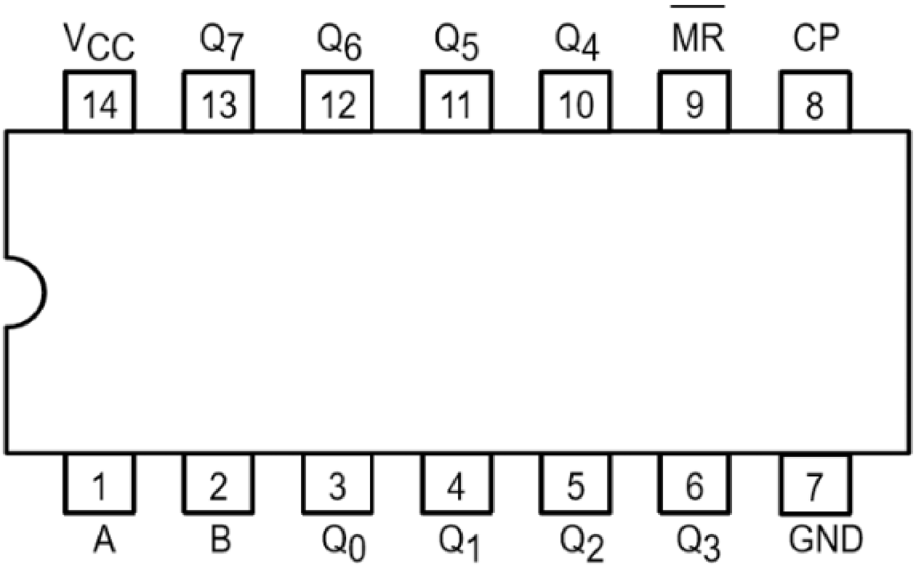
IC74193



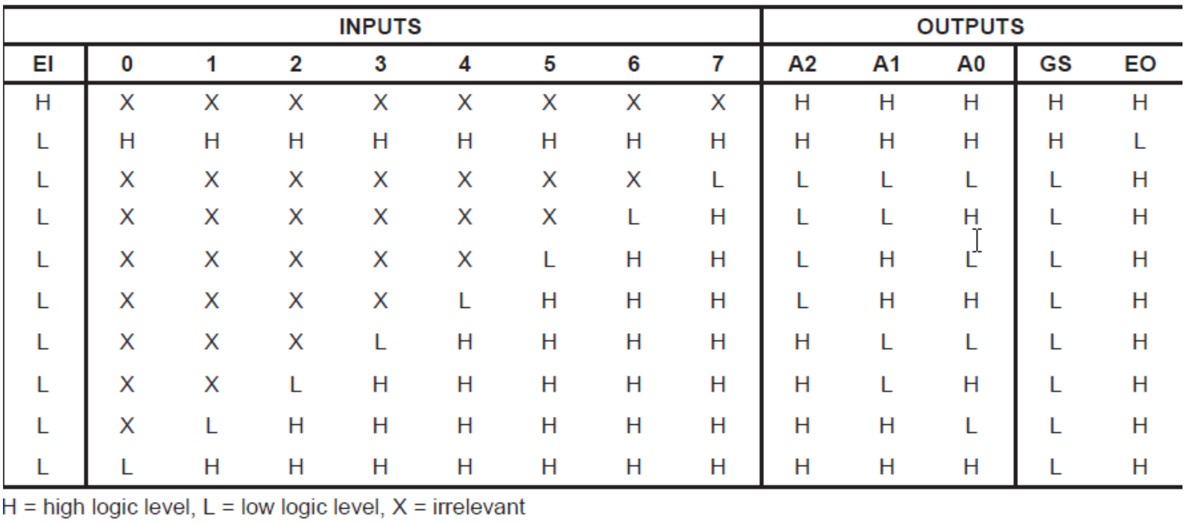


COUNT	OUTPUT			
	Q_0	Q_1	Q_2	Q_3
0	L	L	L	L
1	H	L	L	L
2	L	H	L	L
3	H	H	L	L
4	L	L	H	L
5	H	L	H	L
6	L	H	H	L
7	H	H	H	L
8	L	L	L	H
9	H	L	L	H
10	L	H	L	H
11	H	H	L	H
12	L	L	H	H
13	H	L	H	H
14	L	H	H	H
15	H	H	H	H

IC74164

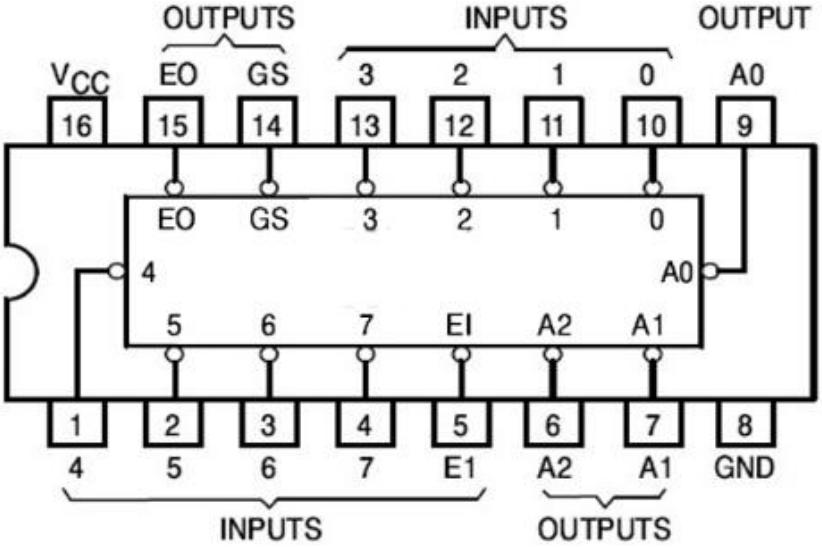


IC74148

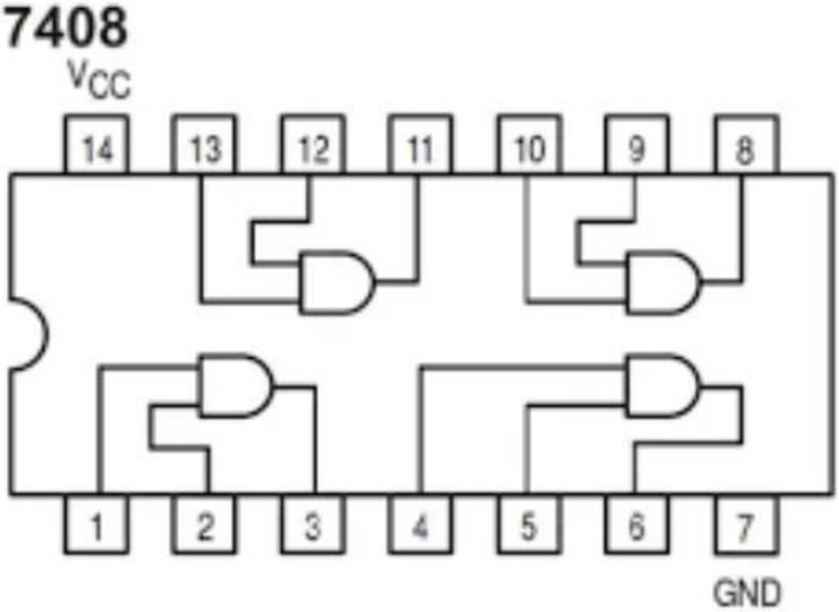


INPUTS									OUTPUTS				
EI	0	1	2	3	4	5	6	7	A2	A1	A0	GS	EO
H	X	X	X	X	X	X	X	X	H	H	H	H	H
L	H	H	H	H	H	H	H	H	H	H	H	H	L
L	X	X	X	X	X	X	X	L	L	L	L	L	H
L	X	X	X	X	X	X	L	H	L	L	H	L	H
L	X	X	X	X	X	L	H	H	L	H	L	L	H
L	X	X	X	X	L	H	H	H	L	H	H	L	H
L	X	X	X	L	H	H	H	H	H	L	L	L	H
L	X	X	L	H	H	H	H	H	H	L	H	L	H
L	X	L	H	H	H	H	H	H	H	H	L	L	H
L	L	H	H	H	H	H	H	H	H	H	H	L	H

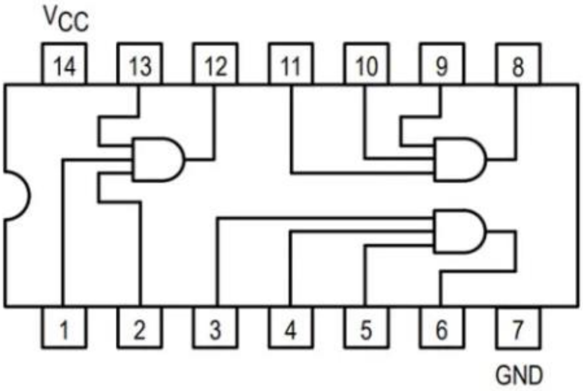
H = high logic level, L = low logic level, X = irrelevant


OUTPUTS
INPUTS
OUTPUT
VCC
EO
GS
3
2
1
0
A0
16
15
14
13
12
11
10
9
EO
GS
3
2
1
0
4
A0
5
6
7
EI
A2
A1
1
2
3
4
5
6
7
8
4
5
6
7
E1
A2
A1
GND
INPUTS
OUTPUTS

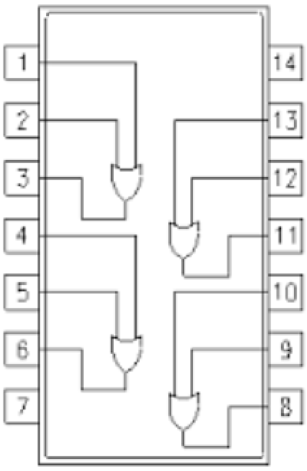
IC7408


7408
VCC
14
13
12
11
10
9
8
1
2
3
4
5
6
7
GND

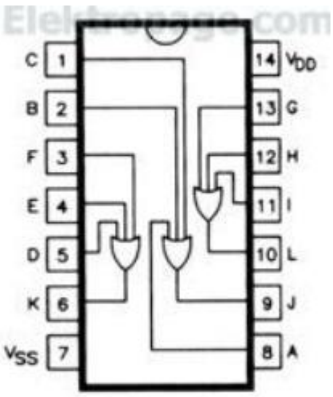
IC7411



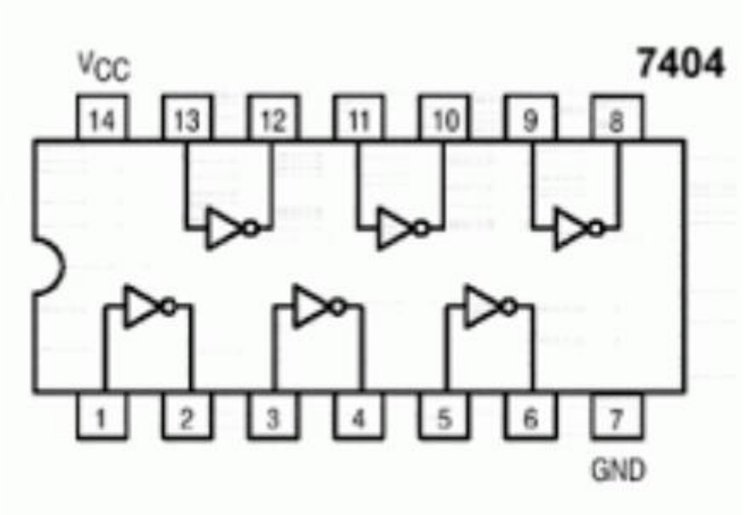
IC7432



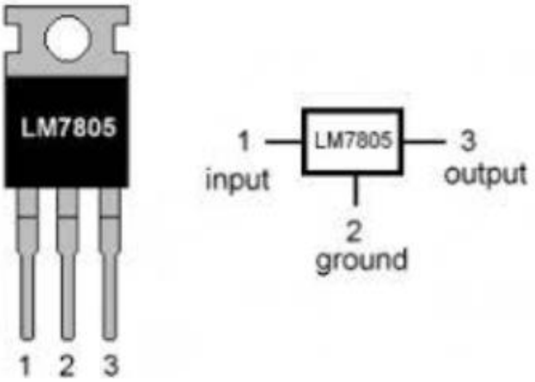
IC4075



IC7404



IC7805



<~~||/\||~~>