CSE260

Digital Logic Design

Lab Project

Project Title: Password security system

Group: 03

Date of submission: 03/01/2022

Submitted by:

Name: Nur-E-Jannat

ID: 21301744

Section: 11 (Lab & Theory)

Name: Kanak Roy Shanda

ID: 21301743

Section: 11 (Lab & Theory)

Introduction

In today's technologically advanced world of the twenty-first century, there is a vital effort for keeping information secure around the world. Now, passwords should not only be essential for storing and securing information, but also for greater security through more verification which will be also comfortable for the owner. The president of Russia Vladimir Putin says, **"**Hackers are free people, just like artists who make up in the morning in a good mood and start painting.**"** Hacking has become so powerful that at any time hackers can match the password with yours. So, it is very vital to secure our personal information from hacking by making a strong and owner-suitable password security system. As a result, we are highly interested in working on the "Password Security System" with two-factor verification.

Objective:

a. To design and implement a circuit that can check that the saved number and the given input number are similar or not by using XNOR gate, AND gate, AND__4 gate, and NOT gate.

b. This circuit diagram helps everyone to become familiar with the hybrid gate(XNOR) and basic gates(AND, NOT).

c. To design the password security design with the two-factor verification code.

Proposed Model

Input:

Consider A as the event of the 8-bit stored password determined by the owner and B as the event of the 8-bit inputted password from the user to enter or log in.

$A = A_7A_6A_5A_4A_3A_2A_1 A_0$
$B = B_7B_6B_5B_4B_3B_2B_1B_0$

- ➢ C=0, it means that the owner doesn't provide any code
- ➢ C=1(decimal 1) means that the owner provides code to log into his or her file for showing

Output:

- ➢ Y = Yellow light
- ➢ G = Green light
- ➢ R = Red light

Condition:

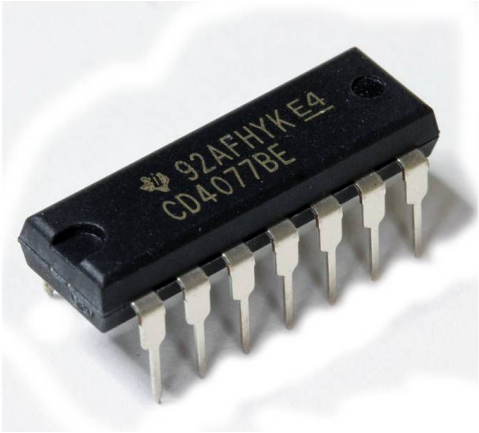
- ➔ Y = 1 means that the stored password and the input password are the same and C = 0. It means that the password is correct and the owner will get a notification;
  Otherwise: 0
- ➔ G = 1 means that the stored password and the input password are correct and the provided code C = 1;
  Otherwise: 0
- ➔ R = 1 means that the stored password and the input password are different and C = 0;
  Otherwise: 0

Experimental Setup

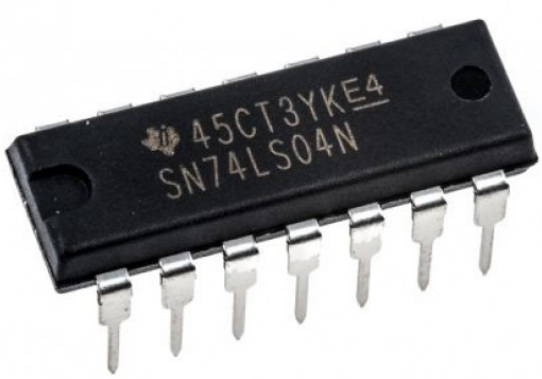
Components

1. 4077(XNOR gate)
2. NOT
3. AND
4. AND_4
5. LED-YELLOW
6. LED-GREEN
7. LED-RED
8. LOGIC PROBE(BIG)
9. LOGICSTATE

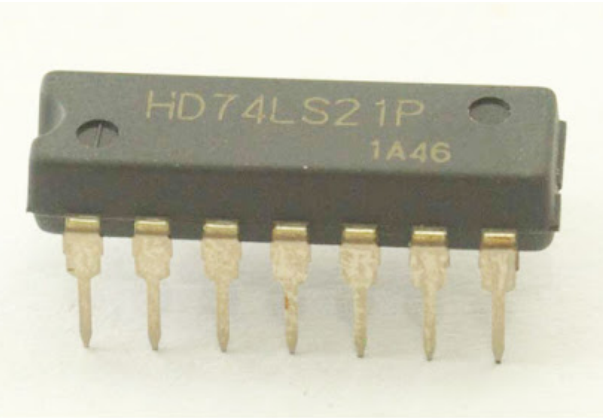
Equipment's:



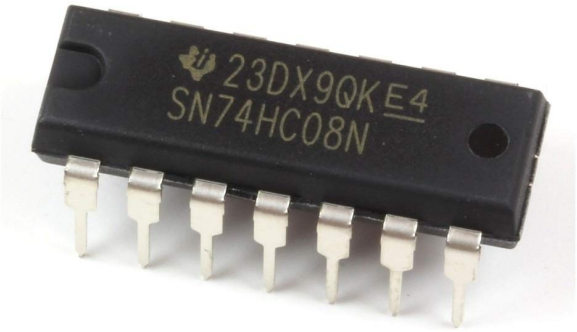
2-input XNOR gate(4077)



NOT gate(7404)

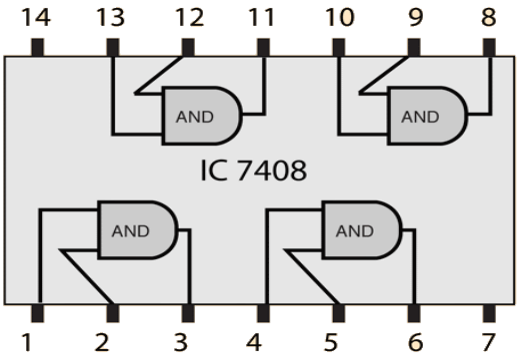


4-Input AND gate(74LS21)

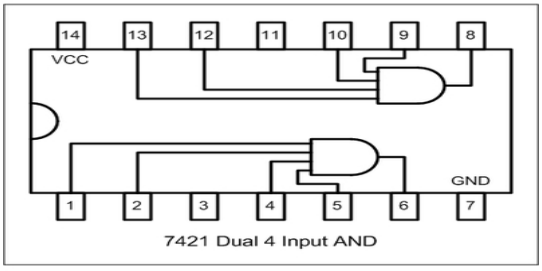


2-Input AND gate(7408)

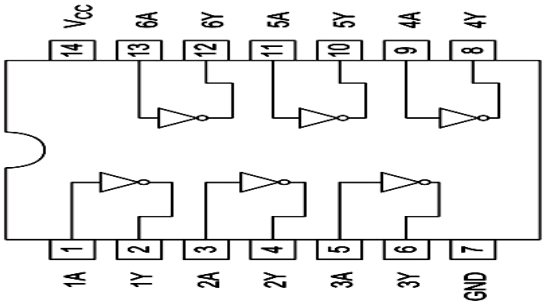
IC Diagram:



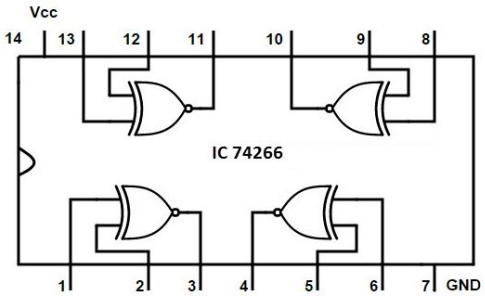
Pin layout of 7408



Pin layout of 74LS21

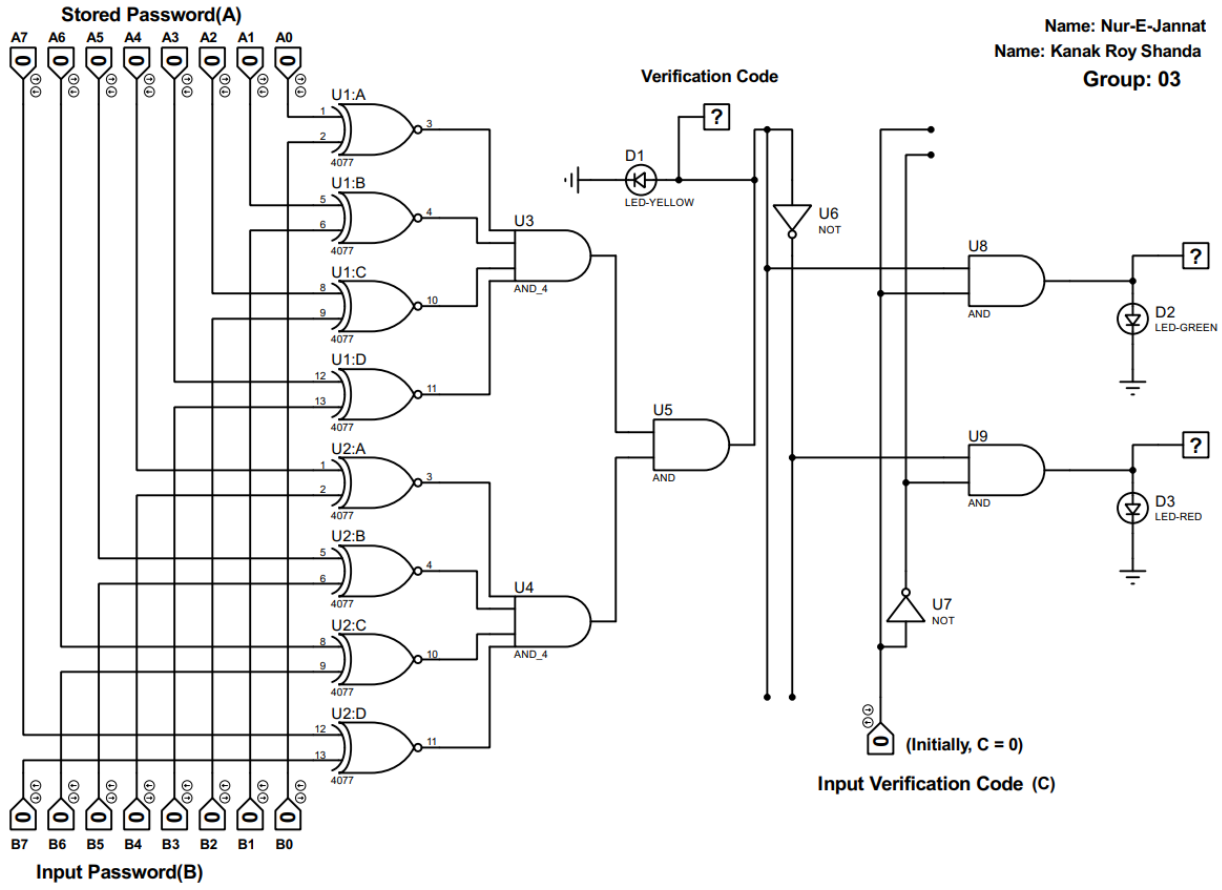


Pin layout of 7404



Pin layout of 4077

Circuit diagram:



Result and Analysis

Procedure:

- ☐ If the stored or fixed password **A($A_7A_6A_5A_4A_3A_2A_1A_0$)** and input password **B($B_7B_6B_5B_4B_3B_2B_1B_0$)** from the user are matched, the **Yellow** light will be "**ON**". As a result, the **Yellow** light indicates that the stored and given password are similar but this isn't final verification. You can't enter into the application or file.

- ☐ Through the notification, a verification code will be sent to the recognizant device. After that, we have to input the verification code where the value of **C** is **1**. Here, C is a one-bit binary number and it is 0 initially**.** When the input verification code will be similar to the given verification code, the **Green** light will be **"ON"**. So, the **Green** light indicates the second verification and you will be able to enter the application or file.

- ☐ If the owner's fixed password **A($A_7A_6A_5A_4A_3A_2A_1A_0$)** and user input **B($B_7B_6B_5B_4B_3B_2B_1B_0$)** are not equal then the **Red** light will **'ON'** directly. Here, the **verification code(C)** is initially **0**. It means our fixed password and users' entered password are not the same bits. There is at least one given a bit that is **different** from the fixed password(A). So, "**Red Light**" indicates that the password is incorrect and the user can't enter the system.

Details for the purpose of understanding the truth table:

In the truth table, First row A=0, B=1, these different bits represent that all bits (eight bits) of the owner set password(A) and user input(B) are not the same. It means at least 1 bit of A($A_7A_6A_5A_4A_3A_2A_1A_0$) and B($B_7B_6B_5B_4B_3B_2B_1B_0$) don't match each other. So, A=0, B=1 represents A≠B.
On the other hand, A=1, B=1 these same bits represent that all bits (eight bits) of the owner set password(A) and user input(B) are the same. It means all the bits of A($A_7A_6A_5A_4A_3A_2A_1A_0$) and B($B_7B_6B_5B_4B_3$ $B_2B_1B_0$) fully match each other. So, A=1,B=1 represent A=B

Truth table:

Input			**Output**		
A=B when A=1, B=1, and A≠B when A=0, B=1					
A(A_7 A_6 A_5 A_4 A_3 A_2 A_1 A_0)	**B(B_7 B_6 B_5 B_4 B_3 B_2 B_1 B_0)**	**C**	**Y**	**G**	**R**
0	**1**	**0**	**0**	**0**	**1**
1	**1**	**0**	**1**	**0**	**0**
1	**1**	**1**	**1**	**1**	**0**

Equations of output:

Y = A B C' + A B C
G = A B C
R = A' B C'

Conclusion

Limitation of this Project:

- ☐ The password security system only works for the 8-bit binary number.
- ☐ If the device for getting the second authentication code is lost anyway, it is not possible to log in.

Concluding remark:

In a nutshell, we have built an 8-bit password security system that is optimal for almost any kind of digital security system. This password security system will help us to protect our important files and social media accounts from other people or hackers. For instance, we can use the 8-bit password security system in bank accounts, companies, applications, digital devices through two-factor authentication. Finally, we tasted different types of variation of 8-bit binary numbers and our system was successfully able to handle all types of variation without any errors.