**Day 20 Notes**

**Creative Day 4**

Example Circuit

My Circuit

Thoughts:

* Make the Pass code user entered rather than hard coded.
* Require changing on first startup
* Store new passcode in EEPROM
* Do I have enough pins to add the 4x4 keypad to the Day 19 Circuit?
  + If so, lets wire that up and use it for the passcode. Function like final Creative Day code where the ascent works when system is unlocked.
  + Else lets use the rotary encoder and the 7 segment display for passcode work, adding push to enter.

Got it—let’s tackle this step-by-step!

### Goals

1. \*\*User-entered Passcode\*\*: The passcode will be user-defined rather than hardcoded, requiring an initial setup on the first startup.

2. \*\*EEPROM Storage\*\*: The passcode should be stored in EEPROM so it persists across power cycles.

3. \*\*Circuit Decision\*\*: Let’s see if you have enough pins for the 4x4 keypad alongside the Day 19 circuit. If not, we’ll use the rotary encoder and 7-segment display as alternatives.

### Step 1: Check Pin Availability for 4x4 Keypad

For the Day 19 circuit, I’ll need to know which components you’re currently using and their pin assignments. However, I can give you a general strategy for determining pin availability:

- \*\*Keypad\*\*: A 4x4 keypad requires 8 pins (4 for rows and 4 for columns).

- \*\*Day 19 Components\*\*: Let me know which components are in use and on which pins. I can suggest alternative pin configurations if you’re short on pins.

If we can fit the keypad into your available pins, we’ll proceed with the wiring and code. If not, we’ll switch to using the \*\*rotary encoder and 7-segment display\*\*.

Could you provide a quick rundown of your Day 19 pin usage? Once we confirm the setup, I’ll guide you through the wiring and code for the passcode entry!

Components and Pin Usage:

Buzzer

Signal (S) -- Pin 10

Ground (-) -- Common Ground Bus

7 Segment Display

CLK -- Pin 6

DIO -- Pin 5

VCC -- Common +5v Bus

GND -- Common Ground Bus

Rotaty Encoder

CLK -- Pin 2

DT -- Pin 3

Power (+) -- Common +5v Bus

GND -- Common Ground Bus

Thanks for the component and pin layout! Based on your current setup, here’s the pin usage analysis for adding the 4x4 keypad:

- \*\*4x4 Keypad\*\*: Requires 8 pins (4 rows + 4 columns).

- \*\*Available Pins\*\*: Your setup is already using \*\*Pins 2, 3, 5, 6, and 10\*\* for the rotary encoder, 7-segment display, and buzzer.

This leaves \*\*Pins 7, 8, 9, 11, 12, and 13\*\* free, which is enough to support the keypad!

Here’s the plan:

### Step 2: Wiring the 4x4 Keypad

Connect the keypad as follows (adjust if your HERO board uses different pin labels for these):

- \*\*Keypad Row Pins (R1-R4)\*\* → Arduino Pins \*\*7, 8, 9, 11\*\*

- \*\*Keypad Column Pins (C1-C4)\*\* → Arduino Pins \*\*12, 13, A0, A1\*\*

With this setup, all components fit, and we have enough pins for the keypad. The next steps involve modifying the code to:

1. Set up and check the passcode.

2. Store and retrieve the passcode from EEPROM.

3. Use the keypad to enter the passcode for system access.

### Step 3: Code for Passcode Setup and Entry

Here’s an outline for the updated code structure:

1. \*\*Passcode Setup and Validation\*\*: Prompts the user to set up a new passcode on the first startup. Stores the new passcode in EEPROM.

2. \*\*Passcode Entry\*\*: After the first startup, retrieves the passcode from EEPROM and requires the user to unlock the system with it.

Would you like the code to proceed with this setup?

#include <Keypad.h>

#include <EEPROM.h>

// Constants for minimum and maximum PIN length

const int minPinLength = 4;

const int maxPinLength = 8;

const int maxAttempts = 5;

const int eepromStartAddress = 0; // EEPROM address for storing PIN

// Keypad setup

const char BUTTONS[4][4] = {

{ '1', '2', '3', 'A' },

{ '4', '5', '6', 'B' },

{ '7', '8', '9', 'C' },

{ '\*', '0', '#', 'D' }

};

const byte ROW\_PINS[4] = { 7, 8, 9, 11 };

const byte COL\_PINS[4] = { 12, 13, A0, A1 };

Keypad heroKeypad = Keypad(makeKeymap(BUTTONS), ROW\_PINS, COL\_PINS, 4, 4);

char currentPIN[maxPinLength + 1]; // Stores the active PIN

int attemptCount = 0;

bool isLocked = true; // System starts in locked state

void setup() {

Serial.begin(9600);

// Load the PIN from EEPROM on startup

if (loadPINFromEEPROM()) {

Serial.println("Stored PIN loaded. Enter PIN to unlock.");

} else {

Serial.println("No PIN found. Set a new PIN (4-8 chars, end with #):");

setupNewPIN();

}

}

void loop() {

if (isLocked) {

Serial.println("System is locked. Enter PIN to unlock:");

if (validatePIN()) {

isLocked = false;

Serial.println("System Unlocked! Options: '#' to lock, '\*' to change PIN, other keys to work.");

} else {

attemptCount++;

if (attemptCount >= maxAttempts) {

Serial.println("Too many failed attempts. System locked.");

while (true); // Lock system permanently

}

}

} else {

char button\_character = heroKeypad.getKey();

if (button\_character) {

if (button\_character == '#') { // Lock system

isLocked = true;

Serial.println("System locked. Enter PIN to unlock.");

} else if (button\_character == '\*') { // Change PIN

Serial.println("Enter current PIN to change:");

if (validatePIN()) {

Serial.println("PIN accepted. Set a new PIN:");

setupNewPIN();

Serial.println("New PIN set. System unlocked.");

} else {

Serial.println("Incorrect PIN. Returning to unlocked state.");

}

} else { // Any other character to "work"

Serial.print("Working... You pressed: ");

Serial.println(button\_character);

}

}

}

}

// Setup a new PIN with verification

void setupNewPIN() {

char tempPIN[maxPinLength + 1];

Serial.println("Enter new PIN:");

if (getPINInput(tempPIN)) {

Serial.println("Re-enter new PIN to confirm:");

char verifyPIN[maxPinLength + 1];

if (getPINInput(verifyPIN) && strcmp(tempPIN, verifyPIN) == 0) {

strcpy(currentPIN, tempPIN);

savePINToEEPROM();

Serial.println("New PIN set successfully!");

} else {

Serial.println("PINs did not match. Restart setup.");

setupNewPIN();

}

}

}

// Save the current PIN to EEPROM

void savePINToEEPROM() {

int length = strlen(currentPIN);

EEPROM.write(eepromStartAddress, length); // Store the length

for (int i = 0; i < length; i++) {

EEPROM.write(eepromStartAddress + 1 + i, currentPIN[i]);

}

}

// Load the PIN from EEPROM

bool loadPINFromEEPROM() {

int length = EEPROM.read(eepromStartAddress);

if (length < minPinLength || length > maxPinLength) {

return false;

}

for (int i = 0; i < length; i++) {

currentPIN[i] = EEPROM.read(eepromStartAddress + 1 + i);

}

currentPIN[length] = '\0';

return true;

}

// Get PIN input with "#" to end entry

bool getPINInput(char\* pinBuffer) {

int charIndex = 0;

while (true) {

char key = heroKeypad.getKey();

if (key) {

if (key == '#') {

pinBuffer[charIndex] = '\0';

if (charIndex >= minPinLength && charIndex <= maxPinLength) {

return true;

} else {

Serial.println("Invalid PIN length. Try again.");

return false;

}

}

if (charIndex < maxPinLength) {

pinBuffer[charIndex] = key;

Serial.print("\*");

charIndex++;

}

}

}

}

// Validate entered PIN against currentPIN

bool validatePIN() {

char enteredPIN[maxPinLength + 1];

if (getPINInput(enteredPIN)) {

if (strcmp(enteredPIN, currentPIN) == 0) {

Serial.println("Access Granted!");

return true;

}

}

Serial.println("Incorrect PIN.");

return false;

}

*~~Test Day 19 – Ascent Code with New Wiring – PASS~~*

*~~Test New Keypad Code – Pass after Correcting Wiring~~*

Let's start by improving the security. Can we wipe the EEPROM PIN when a new program is uploaded.

To automatically wipe the EEPROM when uploading a new program, you can add a simple EEPROM clearing routine that runs only once after the program is uploaded. Here’s a reliable approach:

1. \*\*Define a "Magic Number"\*\* in EEPROM to indicate whether the PIN is valid or not.

2. \*\*Run an EEPROM Clearing Routine\*\* when the program is first uploaded by checking if the stored magic number matches a predefined value.

### Steps

1. \*\*Set Up a Magic Number\*\*:

- Choose an EEPROM address to store a specific "magic number" as a flag indicating the EEPROM data is valid. If the magic number is missing or incorrect (meaning a new program has been uploaded), the program will reset the PIN.

2. \*\*Clear EEPROM on First Run\*\*:

- In `setup()`, check the magic number. If it doesn’t match, clear the EEPROM and set up a new PIN.

### Code Example

Here’s how you can implement this:

```cpp

#include <EEPROM.h>

const int eepromStartAddress = 0; // Starting address for PIN data

const int magicNumberAddress = 100; // Separate address to store the magic number

const int magicNumber = 1234; // Arbitrary number to flag valid EEPROM data

void setup() {

Serial.begin(9600);

// Check if magic number exists; if not, clear EEPROM

int storedMagic = EEPROM.read(magicNumberAddress);

if (storedMagic != magicNumber) {

Serial.println("New program detected. Clearing EEPROM...");

clearEEPROM();

EEPROM.write(magicNumberAddress, magicNumber); // Set the magic number after clearing

} else {

Serial.println("Valid EEPROM data found.");

}

// Rest of your setup code here

}

void clearEEPROM() {

for (int i = eepromStartAddress; i < EEPROM.length(); i++) {

EEPROM.write(i, 0); // Set each byte in EEPROM to 0

}

}

```

### Explanation

- \*\*Magic Number Check\*\*: On startup, the program reads the stored magic number from EEPROM. If it doesn’t match the expected value (`1234`), it assumes this is the first run after a new upload.

- \*\*Clear EEPROM\*\*: If a mismatch is found, `clearEEPROM()` sets each EEPROM address to 0, wiping all saved data.

- \*\*Write Magic Number\*\*: After clearing, the program writes the magic number to EEPROM so it knows next time that the data is valid.

This approach will ensure that your PIN and other data are reset with each new program upload, enhancing security by not retaining stale data. Let me know how it goes, or if you’d like more adjustments!

Can you integrate this code snip with the keypad code just tested?

Here’s the updated code that integrates the \*\*EEPROM clearing\*\* functionality into the previously tested \*\*keypad passcode setup and validation\*\* code. This version checks for a magic number in EEPROM on startup, and if the magic number isn’t present, it clears the EEPROM and requires a new PIN setup.

### Integrated Code

```cpp

#include <Keypad.h>

#include <EEPROM.h>

// Constants for minimum and maximum PIN length

const int minPinLength = 4;

const int maxPinLength = 8;

const int maxAttempts = 5;

const int eepromStartAddress = 0; // EEPROM start address for PIN

const int magicNumberAddress = 100; // EEPROM address for magic number

const int magicNumber = 1234; // Unique number to flag valid EEPROM data

// Keypad setup

const char BUTTONS[4][4] = {

{ '1', '2', '3', 'A' },

{ '4', '5', '6', 'B' },

{ '7', '8', '9', 'C' },

{ '\*', '0', '#', 'D' }

};

const byte ROW\_PINS[4] = { 7, 8, 9, 11 };

const byte COL\_PINS[4] = { 12, 13, A0, A1 };

Keypad heroKeypad = Keypad(makeKeymap(BUTTONS), ROW\_PINS, COL\_PINS, 4, 4);

char currentPIN[maxPinLength + 1]; // Stores the active PIN

int attemptCount = 0;

bool isLocked = true; // System starts in locked state

void setup() {

Serial.begin(9600);

// Check if magic number is in EEPROM; if not, clear EEPROM and require new PIN

if (EEPROM.read(magicNumberAddress) != magicNumber) {

Serial.println("New program detected. Clearing EEPROM...");

clearEEPROM();

EEPROM.write(magicNumberAddress, magicNumber); // Store the magic number after clearing

Serial.println("No PIN found. Set a new PIN (4-8 chars, end with #):");

setupNewPIN();

} else {

Serial.println("Stored PIN loaded. Enter PIN to unlock.");

loadPINFromEEPROM();

}

}

void loop() {

if (isLocked) {

Serial.println("System is locked. Enter PIN to unlock:");

if (validatePIN()) {

isLocked = false;

Serial.println("System Unlocked! Options: '#' to lock, '\*' to change PIN, other keys to work.");

} else {

attemptCount++;

if (attemptCount >= maxAttempts) {

Serial.println("Too many failed attempts. System locked.");

while (true); // Lock system permanently

}

}

} else {

char button\_character = heroKeypad.getKey();

if (button\_character) {

if (button\_character == '#') { // Lock system

isLocked = true;

Serial.println("System locked. Enter PIN to unlock.");

} else if (button\_character == '\*') { // Change PIN

Serial.println("Enter current PIN to change:");

if (validatePIN()) {

Serial.println("PIN accepted. Set a new PIN:");

setupNewPIN();

Serial.println("New PIN set. System unlocked.");

} else {

Serial.println("Incorrect PIN. Returning to unlocked state.");

}

} else { // Any other character to "work"

Serial.print("Working... You pressed: ");

Serial.println(button\_character);

}

}

}

}

// Set up a new PIN with verification

void setupNewPIN() {

char tempPIN[maxPinLength + 1];

Serial.println("Enter new PIN:");

if (getPINInput(tempPIN)) {

Serial.println("Re-enter new PIN to confirm:");

char verifyPIN[maxPinLength + 1];

if (getPINInput(verifyPIN) && strcmp(tempPIN, verifyPIN) == 0) {

strcpy(currentPIN, tempPIN);

savePINToEEPROM();

Serial.println("New PIN set successfully!");

} else {

Serial.println("PINs did not match. Restart setup.");

setupNewPIN();

}

}

}

// Save the current PIN to EEPROM

void savePINToEEPROM() {

int length = strlen(currentPIN);

EEPROM.write(eepromStartAddress, length); // Store the length

for (int i = 0; i < length; i++) {

EEPROM.write(eepromStartAddress + 1 + i, currentPIN[i]);

}

}

// Load the PIN from EEPROM

bool loadPINFromEEPROM() {

int length = EEPROM.read(eepromStartAddress);

if (length < minPinLength || length > maxPinLength) {

return false;

}

for (int i = 0; i < length; i++) {

currentPIN[i] = EEPROM.read(eepromStartAddress + 1 + i);

}

currentPIN[length] = '\0';

return true;

}

// Clear the EEPROM (reset all bytes to 0)

void clearEEPROM() {

for (int i = eepromStartAddress; i < EEPROM.length(); i++) {

EEPROM.write(i, 0); // Reset each byte in EEPROM to 0

}

}

// Get PIN input with "#" to end entry

bool getPINInput(char\* pinBuffer) {

int charIndex = 0;

while (true) {

char key = heroKeypad.getKey();

if (key) {

if (key == '#') {

pinBuffer[charIndex] = '\0';

if (charIndex >= minPinLength && charIndex <= maxPinLength) {

return true;

} else {

Serial.println("Invalid PIN length. Try again.");

return false;

}

}

if (charIndex < maxPinLength) {

pinBuffer[charIndex] = key;

Serial.print("\*");

charIndex++;

}

}

}

}

// Validate entered PIN against currentPIN

bool validatePIN() {

char enteredPIN[maxPinLength + 1];

if (getPINInput(enteredPIN)) {

if (strcmp(enteredPIN, currentPIN) == 0) {

Serial.println("Access Granted!");

return true;

}

}

Serial.println("Incorrect PIN.");

return false;

}

```

### Explanation of Integrated Changes

1. \*\*Clear EEPROM on New Upload\*\*:

- The `magicNumberAddress` in EEPROM stores a unique number (`magicNumber = 1234`).

- On startup, the code checks if the magic number matches. If not, `clearEEPROM()` is called, resetting all EEPROM addresses to 0.

- After clearing, the magic number is stored to signal that the EEPROM now contains valid data.

2. \*\*First-Time Setup\*\*:

- If the EEPROM is cleared (no valid magic number), the program will prompt the user to set a new PIN.

- After the initial setup, `savePINToEEPROM()` writes the PIN to EEPROM for future use.

3. \*\*Load PIN from EEPROM\*\*:

- On subsequent startups, the program reads the stored PIN from EEPROM if the magic number matches.

### Testing Tips

1. \*\*Verify First-Run Behavior\*\*: Upload the program and check that it prompts for a new PIN, then stores it along with the magic number.

2. \*\*Subsequent Starts\*\*: After setting the PIN, re-upload the code without changing the magic number, and confirm that the PIN persists.

3. \*\*Magic Number Changes\*\*: To simulate a “new program” upload, change `magicNumber` to another value, triggering a new PIN setup on the next upload.

This should ensure your system resets the PIN on new uploads, enhancing security. Let me know if this works as expected or if further tweaks are needed!