Mini Enigma Machine

Autor: Cătălin-Alexandru Rîpanu

Grupă: 333CC

Introducere

Ce face?

Mașina Enigma reprezintă o unitate electro-mecanică bazată pe codul Morse cu suport criptografic ce a fost implementată și folosită de către Germania Nazistă cu scopul de a transmite mesaje critice criptate cu ajutorul unui algoritm complex ce se credea a fi imposibil de spart (imbatabil), bazat pe plugboard și rotoare.

Proiectul constă în implementarea și proiectarea unui nou model de mașină Engima ce implică funcționalități deja existente în cadrul versiunii clasice și funcționalități noi care facilitează transmiterea de mesaje text, în clar, prin Bluetooth, și întoarcerea lor, de către mașină, în varianta criptată.

Scopul și utilitatea proiectului

Această temă are rolul de a prezenta creativitatea tehnică de care au dat dovadă inginerii din Germania Nazistă atunci când au proiectat, în jurul anului 1918, algoritmul de criptare bazat pe componentele fizice ale mașinii, cum ar fi lămpile și rotoarele. Mai mult, acest proiect ar putea face parte din studiul creării unui nou algoritm, eventual cuantic, criptografic, ce îl extinde pe cel curent, folosind tehnici clasice sau din paradigma Quantum.

Ideea de la care am pornit

Inițial, am vrut să înțeleg și să analizez mai multe despre cum funcționează algoritmul Enigma, prin urmare am decis să implementez eu o versiune proprie pentru a îndeplini acest lucru. De asemenea, am citit anumite documentații bazate pe această temă care explicau, clar și concis, fundamentele matematice care stau la baza logicii întregului algoritm, așa că dorința de a aborda acest proiect s-a amplificat.

Descriere generală

După pornirea și inițializarea Enigmei, inițial, utilizatorul va putea să aleagă între 2 moduri de criptare: criptare folosind interfața grafică și criptare folosind transmisia unui mesaj prin Bluetooth. Indiferent de varianta aleasă, mașina va întoarce același rezultat, și anume mesajul criptat.

Folosind un display LCD TFT (touchscreen) compatibil cu placa Arduino UNO, ce cuprinde și un slot pentru un card SD, se va expune o interfață grafică ce va simula unitatea centrală / panoul central de comandă cu toate componentele aferente versiunii clasice (lămpi, tastatură, rotoare, etc).

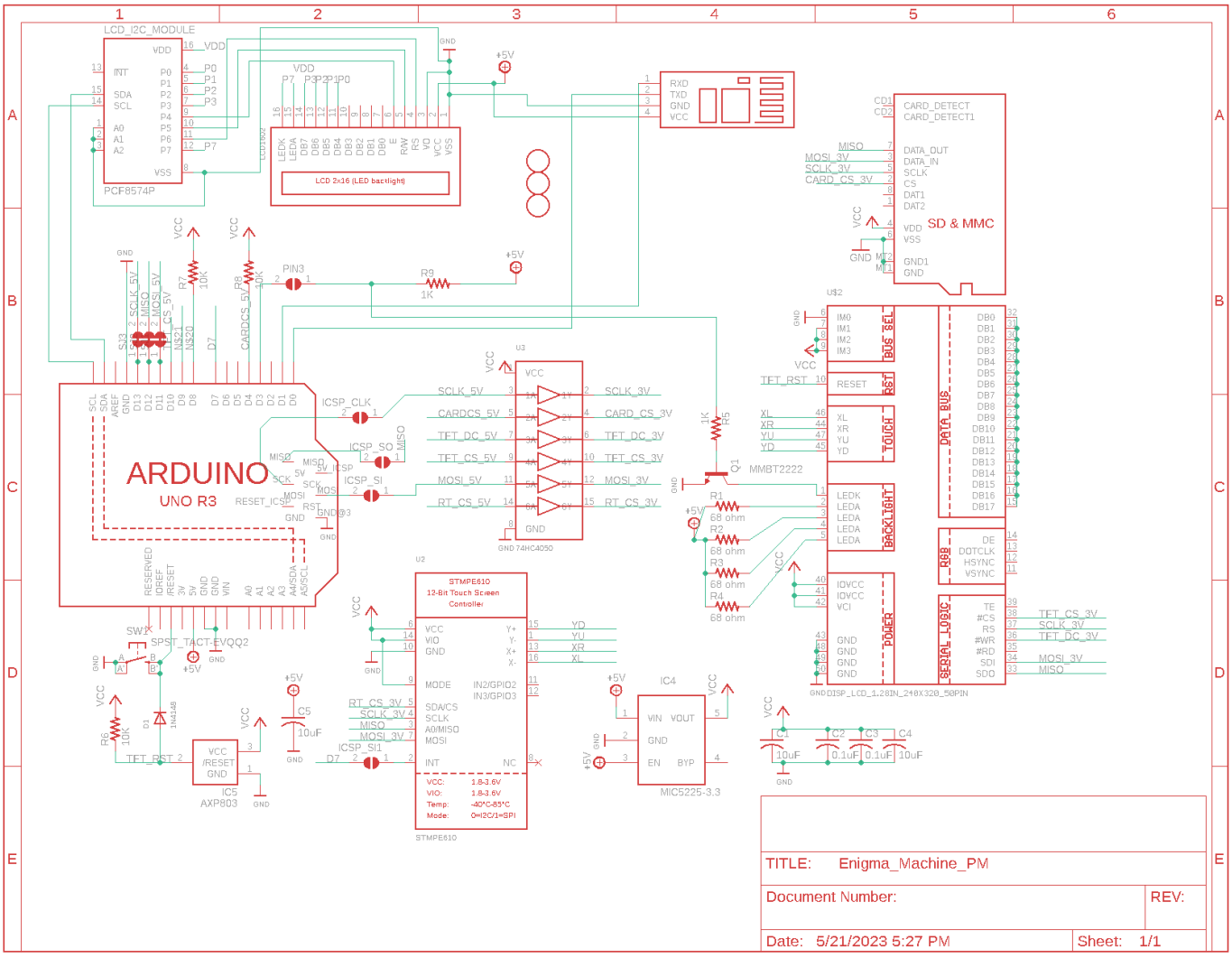
Această variantă de mașină reprezintă, în esență, o versiune portabilă a mașinii reale ce îndeplinește același rol care asigură ridicarea gradului de securitate în cadrul unei comunicații ce se stabilește între 2 entități.

Schemă Bloc

Hardware Design

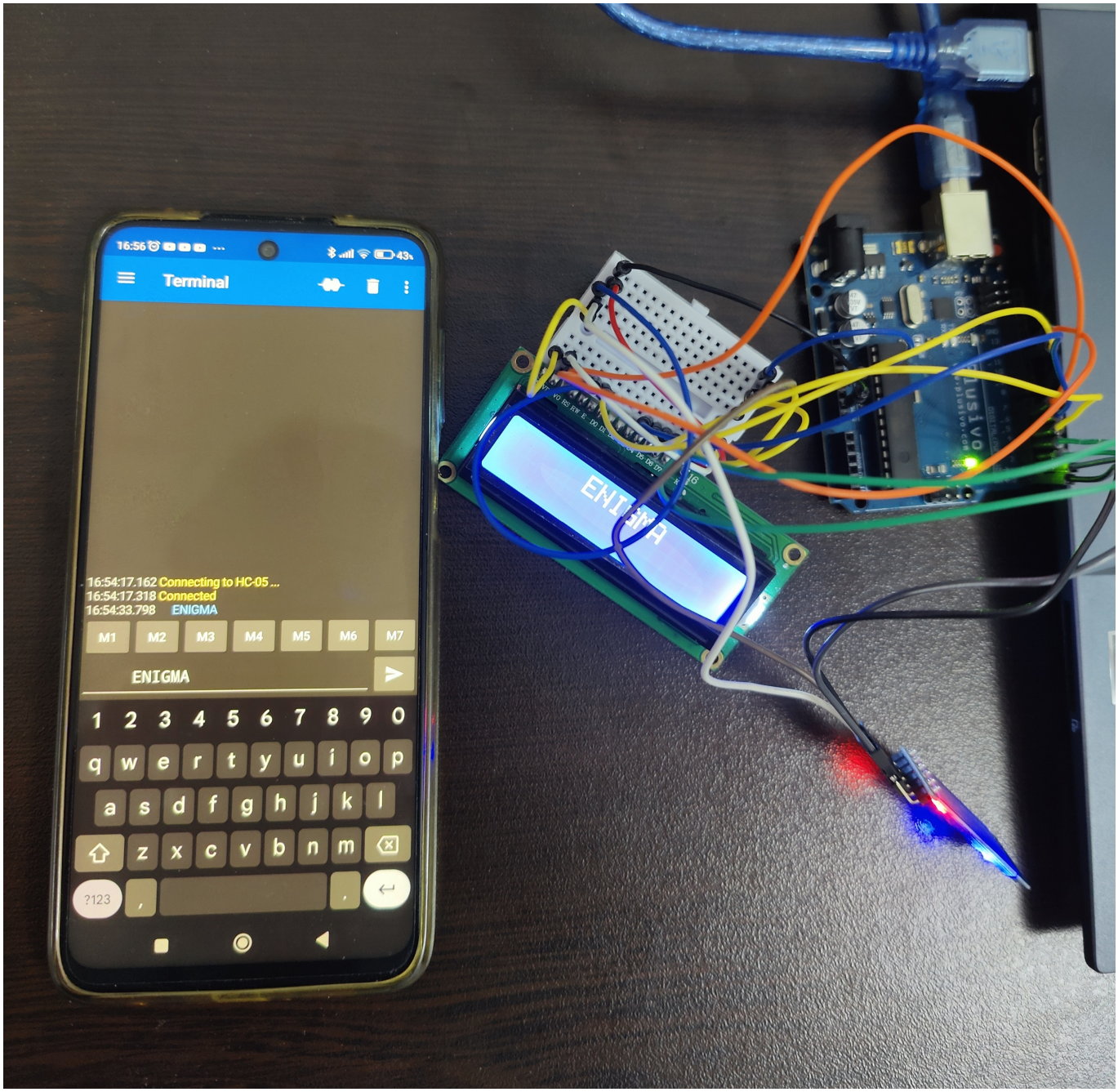
- Arduino UNO R3
- Display LCD Adafruit TFT 2.8”
- Fire jumper male / female
- Modul Bluetooth HC-05
- Modul I2C pentru LCD 1602
- Mini Breadboard
- Mufă Baterie 9V
- Baterie 9V
- Carcasă
- LCD 1602

Schema Electrică



Inițializarea Proiectului


ENIGMA
Enigma Machine
v1.0
Catalin Riparu
PM Project 2022-2023
Soon to be finished.
Tap anywhere to
begin...



Software Design

Software-ul proiectului a fost efectuat folosind mediul de dezvoltare **Arduino IDE**, versiunea 2.1.0.

Bibliotecile folosite în cadrul proiectului sunt următoarele:

- **#include <SPI.h>**, pentru a putea comunica și opera cu LCD-ul TouchScreen TFT.

- **#include <LiquidCrystal_I2C.h>**, pentru a putea manipula modulul I2C care se ocupa de LCD-ul 1602.

- **#include <Adafruit_ILI9341.h>**, pentru a putea realiza transferul de date către / de la LCD-ul TFT (interfațare).

- **#include <Adafruit_STMPE610.h>**, pentru a putea citi de pe chip coordonatele (x,y) ale zonei apăsate.

- **#include <Adafruit_GFX.h>**, pentru a putea realiza și afișa obiecte / artefacte grafice destinate LCD-ului TFT.

Operare:

1. Pornire:

- din ecranul de pornire, se poate atinge oriunde LCD-ul TFT pentru a merge spre simularea Enigmei.

- simularea începe cu standardul M3 Enigma (1939) ce folosește reflectorul B, împreună cu roțile standard III, II și I.

- roțile montate au inelele puse în pozițiile implicite, fără a avea fire conectate în cadrul plugboard-ului (partea de jos).

- pentru a schimba arhitectura mașinii curente, se poate apăsa pe logo-ul din dreapta sus. Se va afișa pagina de configurare.

- pentru a șterge datele de ieșire, se apasă pe bandă.

- pentru a modifica literele rotoarelor, se poate apăsa pe partea superioară / inferioară a respectivului rotor. Partea superioară afișează litera ce se află înaintea literei curente (ordinea alfabetică), iar partea inferioară afișează litera ce se află după litera curentă (ordinea alfabetică).

2. Configurare:

- simulatorul permite următoarele configurații standard:

1. Standard M3 1939
    1. Tipul Mașinii: Enigma M3 (1939)
    2. Reflectorul: B
    3. Lungime grup: 5
    4. Roți: III II I
    5. Inele: 01 01 01
    6. Fire: (fără fire)
2. Rocket K Railway
    1. Tipul Mașinii: Enigma Rocket K Railway
    2. Reflectorul: A
    3. Lungime grup: 5
    4. Roți: III II I
    5. Inele: 01 01 01 01
    6. Fire: (fără plugboard)
3. Turing Rocket K 1940
    1. Tipul Mașinii: Enigma Rocket K Railway
    2. Reflectorul: A
    3. Lungime grup: 5
    4. Roți: III I II
    5. Inele: 26 17 16 13
    6. Fire: (fără plugboard)
4. Barbarosa M3 1941

1. Tipul Mașinii: Enigma M3 (1939)
2. Reflectorul: B
3. Lungime grup: 5
4. Roți: II IV V
5. Inele: 02 21 12
6. Fire: AV BS CG DL FU HZ IN KM OW RX

5. Standard M4 1942
   1. Tipul Mașinii: Enigma M4 (1942)
   2. Reflectorul: Thin B
   3. Lungime grup: 4
   4. Roți: B III II I
   5. Inele: 01 01 01 01
   6. Fire: (fără fire)
6. Scharnhorst M3 1943
   1. Tipul Mașinii: Enigma M3 (1939)
   2. Reflectorul: B
   3. Lungime grup: 5
   4. Roți: III VI VIII
   5. Inele: 01 08 13
   6. Fire: AN EZ HK IJ LR MQ OT PV SW UX

- pentru a selecta o configurare specifică, se poate apăsa pe butonul “Quick Setup”. La fiecare apăsare, se va avansa în listă.

- când s-a ajuns la configurația dorită, aceasta poate fi încărcată apăsând butonul “LOAD”. **Atenție**, acest buton doar afișează configurația, nu o face și activă.

- evident, pentru a seta o anumită componentă (fir, inel, roată, etc) trebuie apăsată zona albastră din dreptul componentei respective (fiecare apăsare va afișa următorul element suportat din listă).

- grupul (tape-ul) se referă la separarea literelor criptate / decriptate pe grupuri ce au lungimea configurabilă din interfață.

- pentru a putea activa o setare făcută, se apasă pe butonul “ACTIVATE”. Evident, pentru a renunța la noua setare și păstra vechea setare, se apasă pe butonul “DISCARD”.

- literele legate prin fire vor fi colorate în mov și, pentru fiecare literă, se va afișa perechea sa (în partea de jos a literei respective).

3. Bluetooth

- acest simulator suportă și operarea cu protocolul de comunicație Bluetooth.

- după ce se părăsește pagina de configurare, se va afișa o nouă pagină care solicită alegerea unui mod de operare (clasic sau Bluetooth).

- dacă se alege varianta clasică, mașina poate primi date de intrare doar prin intermediul tastaturii.

- dacă se alege varianta Bluetooth, mașina poate primi date și prin intermediul interfeței seriale ce este folosită de orice aplicație Bluetooth pentru Android (se recomandă aplicația Serial Bluetooth Terminal 1.43 disponibilă pe **Play Store** întrucât a fost testată în cadrul dezvoltării proiectului). Conectarea se realizează cu ajutorul modulului HC-05.

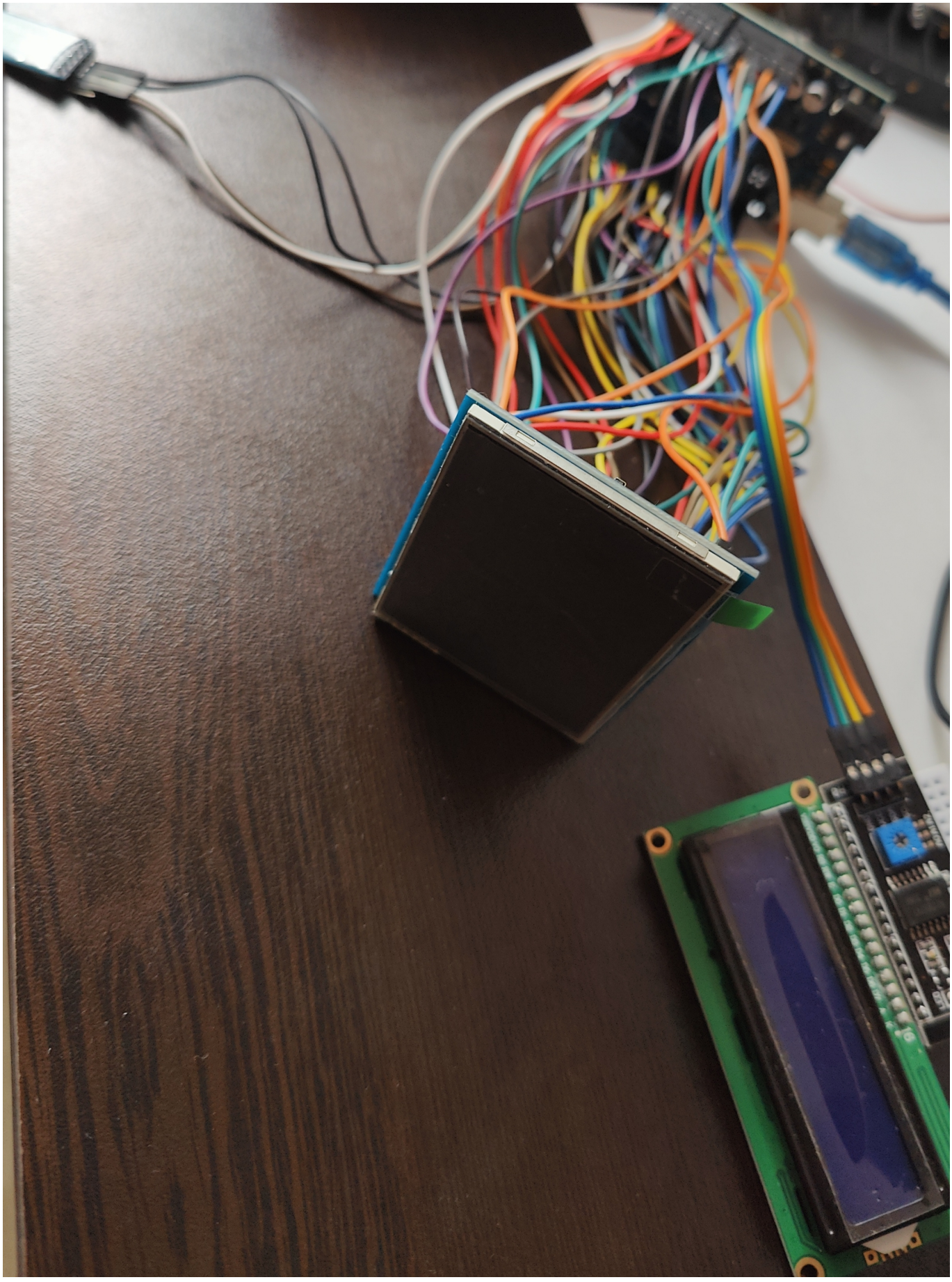
- evident, și în acest mod, mașina poate primi date prin intermediul tastaturii.

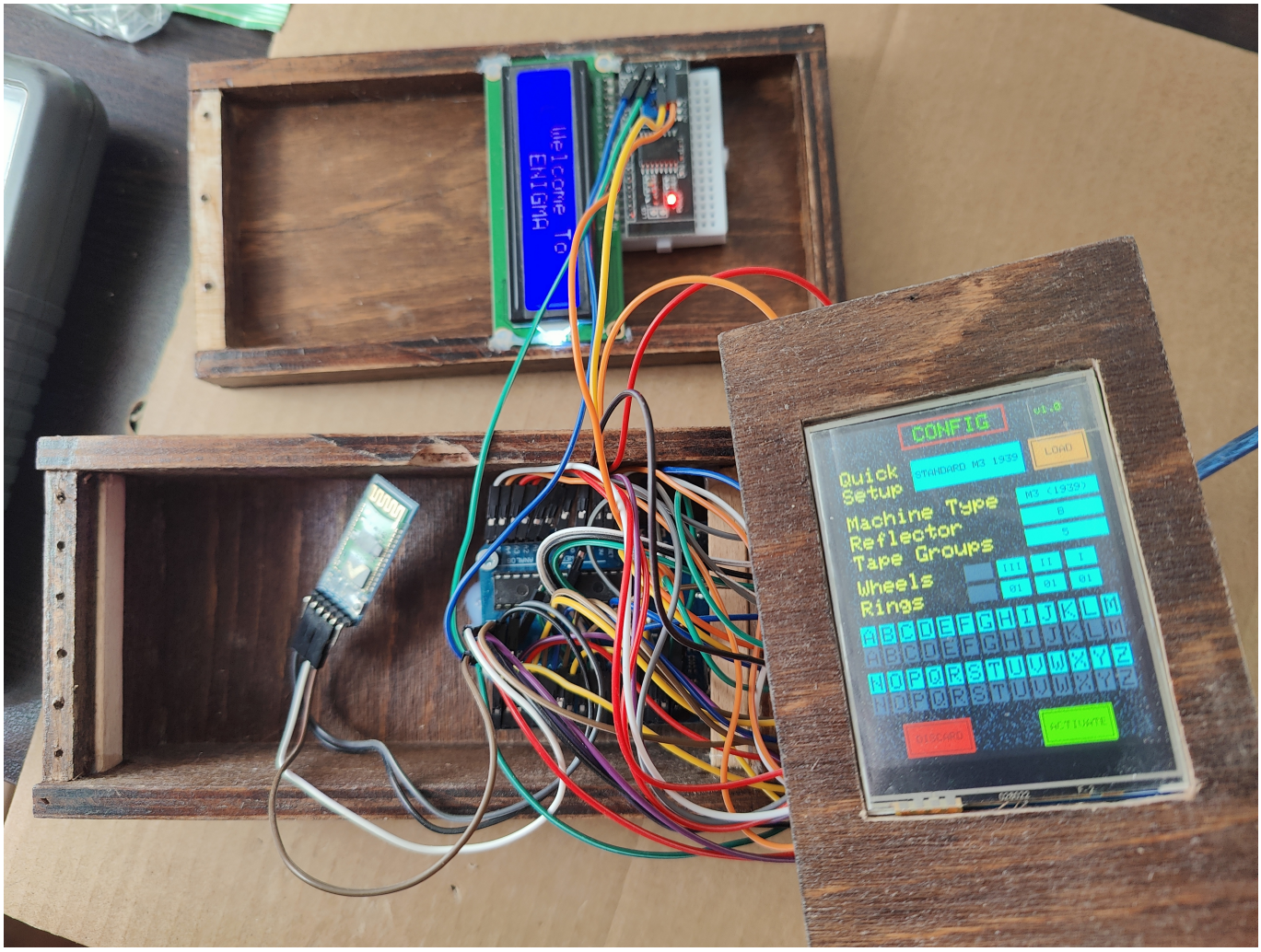
- pentru a vedea dacă modul Bluetooth este activat, se afișează un text verde (“Bluetooth”) în colțul din stânga sus. Dacă acesta nu mai este, înseamnă că este activat modul clasic de operare.

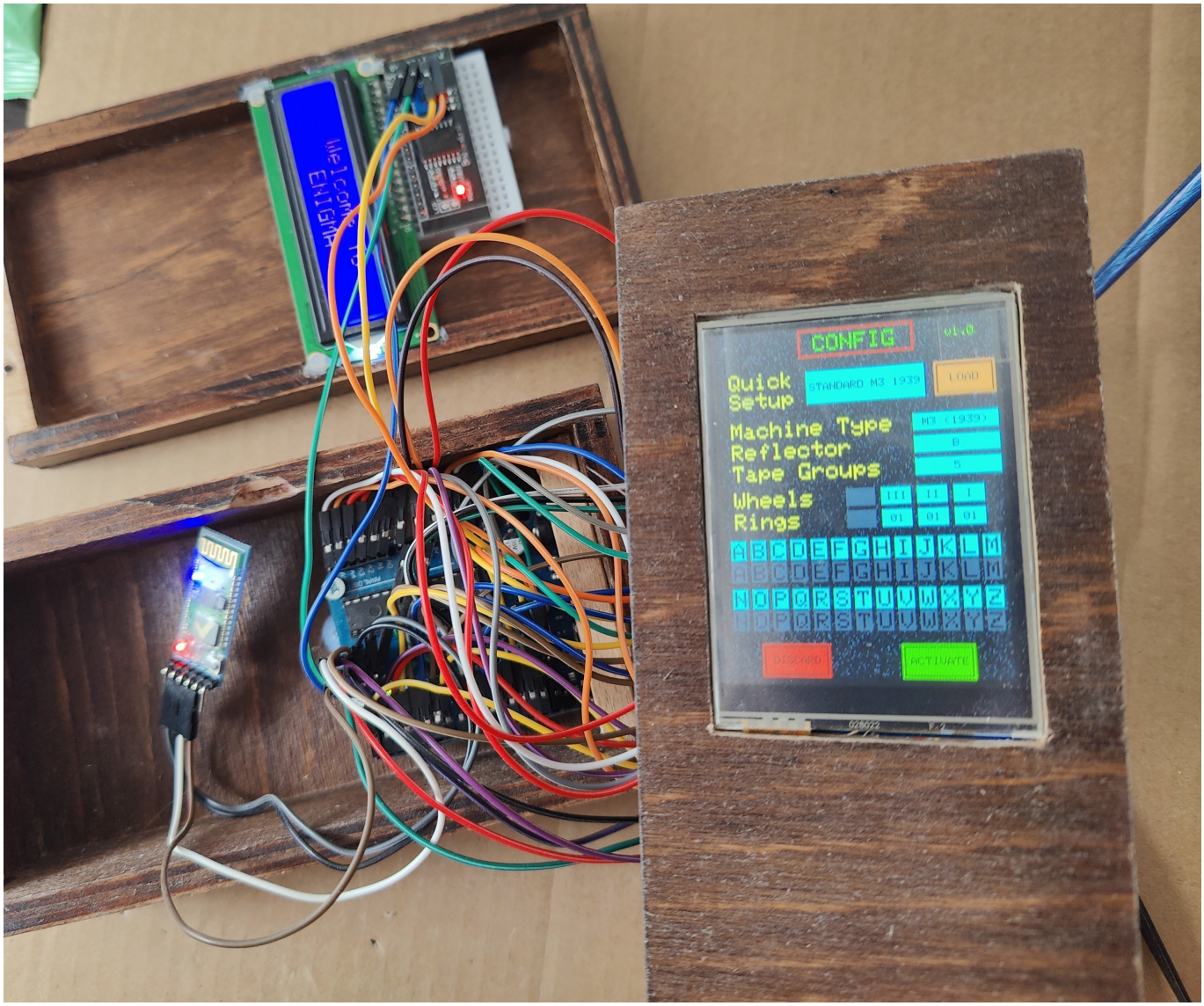
- dacă se încearcă transmiterea de date prin intermediul Bluetooth-ului atunci când acest mod este dezactivat, mașina nu va cripta / decripta ceea ce s-a introdus, dar va păstra intr-o zonă de memorie informația (cu alte cuvinte, dacă se va activa modul Bluetooth imediat după transmiterea datelor, mașina o să pornească procesul de prelucrare).

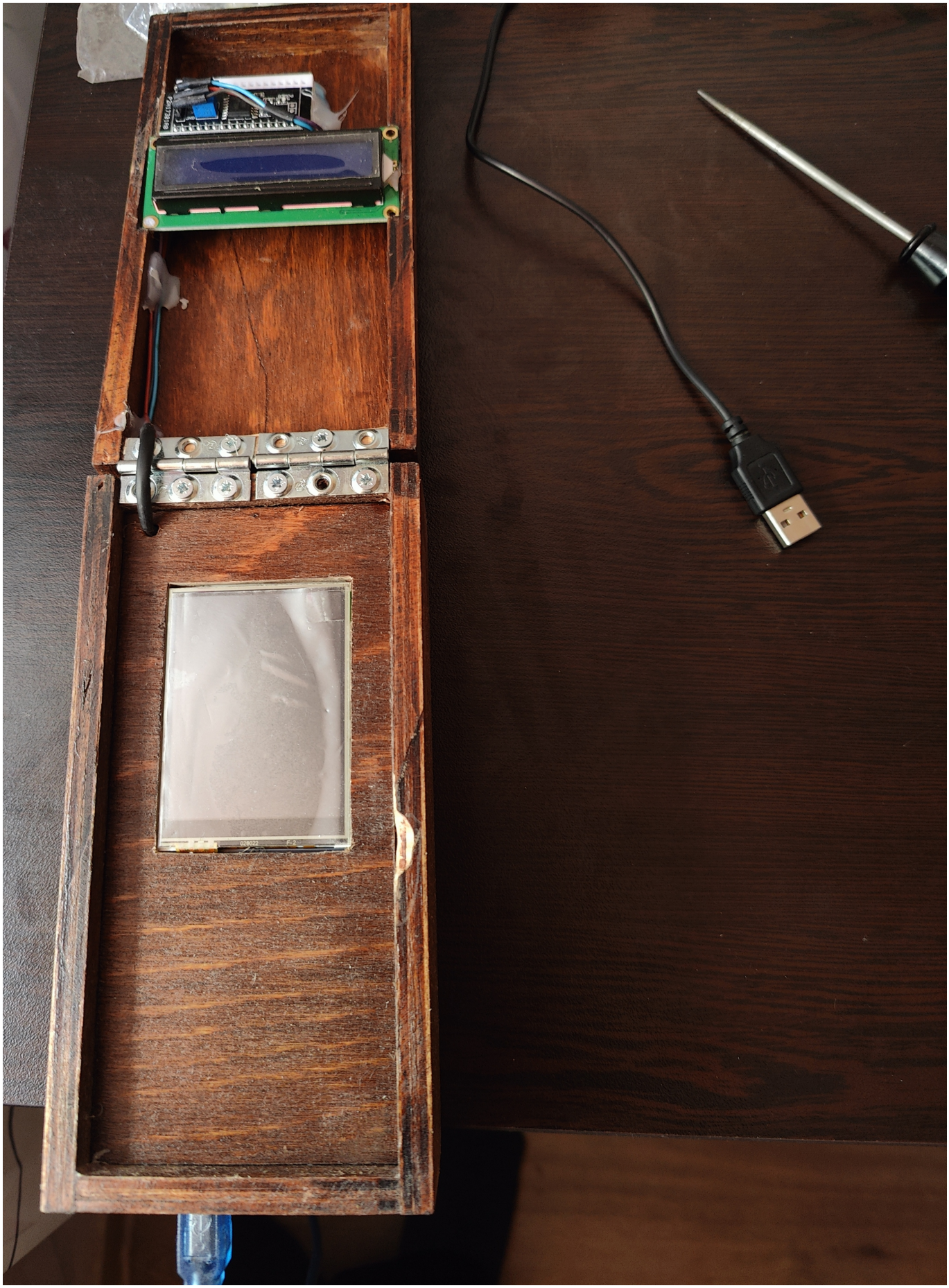
- pentru a curăța banda prin Bluetooth, se folosește caracterul '*'.

Rezultate Obţinute




Welcome To
ENIGMA
CONFIG
v1.0
Quick Setup
STANDARD M3 1939
LOAD
Machine Type
M3 (1939)
Reflector
B
Tape Groups
5
Wheels
III II I
Rings
01 01 01
DISCARD
SETTINGS


CONFIG
v1.0
Quick Setup
STANDARD M3 1939
LOAD
Machine Type
M3 (1939)
Reflector
B
Tape Groups
5
Wheels
III II I
Rings
01 01 01
DISCARD
ACTIVATE



Concluzii

A fost o experiență interesantă, evident, având în vedere că proiectul a reprezentat, de fapt, o dualitate Hardware & Software, care necesită o anumită abordare (biblioteci compatibile cu resursele Hardware, componente compatibile cu alte componente, etc). La începutul proiectului am schimbat ecranul LCD TFT (luasem un model din China) întrucât, efectiv, nu mergeau bibliotecile cu suport grafic de la **Adafruit**. De asemenea, formarea cutiei din lemn a reprezentat o problemă pe parcurs, am avut puțin noroc spre final întrucât am găsit un tâmplar care a acceptat lucrarea propusă în urma vizualizării fișei tehnice oferite. O etapă dificilă a reprezentat montarea tuturor modulelor în cutie (a trebuit să fac niște lipituri astfel încât LCD-ul 1602 și modulul I2C să funcționeze, un vecin cunoscut mi-a oferit pistolul său de lipit). Partea cea mai provocatoarea a fost scrierea Software-ului, în fișierul din arhiva .zip sunt, aproximativ, în jur de 3500 de linii de cod (nu am putut reduce cu mult acest număr, mai mult, am avut probleme și cu etapa de compilare uneori întrucât IDE-ul îmi tot spunea că depășesc cei 32KB destinați memoriei Flash de pe placă, în prezent implementarea ocupă o memorie de ~ 32212 bytes din 32256 bytes).

În final, mă bucur că am reușit să obțin propria variantă de **mașină Enigma**.

Download

Pentru permisiunea accesului codului sursă, puteți trimite un mesaj la adresa de email catalin.ripanu@stud.acs.upb.ro.

Jurnal

6.05.2023: S-a postat pagina aferentă proiectului Enigma.

7.05.2023: S-au actualizat descrierile și componentele hardware, alături de schema bloc.

21.05.2023: S-a postat schema electrică aferentă. De asemenea, s-au postat și câteva poze ale proiectului.

29.05.2023: S-au postat informațiile aferente etapei Software și câteva imagini cu progresul Hardware. Proiectul a fost finalizat.

Bibliografie/Resurse

- http://people.physik.hu-berlin.de/~palloks/js/enigma/index_en.html → cel mai important link, conține aplicația care m-a ajutat cu **Proiectarea Algoritmilor** din spatele **Enigmei**.

- https://www.stephenpeek.co.uk/enigma_machines.htm

- https://lastminuteengineers.com/i2c-lcd-arduino-tutorial/

- https://github.com/adafruit/Adafruit-GFX-Library

- https://learn.adafruit.com/adafruit-2-8-tft-touch-shield-v2/overview

- https://cdn-shop.adafruit.com/datasheets/STMPE610.pdf

- https://cdn-shop.adafruit.com/datasheets/ILI9341.pdf

- https://cdn-shop.adafruit.com/datasheets/MI0283QT-11%20V1.1.PDF

- https://ocw.cs.pub.ro/courses/pm → laboratoarele de PM.

Export to PDF