Enigma

Cílem toho projektu byla implementace šifrovacího stroje **Enigma** pro MCU FITkitu. Variant tohoto stroje existuje několik. Tato implementace využívá variantu, jejíž model leží v *Bletchley Park Museum* [1]

1 Popis ovládání

Ovládání probíhá pomocí připojené 4x4 klávesnice FITkitu, kde se číselník chová stejně jako na tlačítkových mobilních telefonech - tzn. první stisk vygeneruje dané číslo, další následující stisky generují jedno z písmen přiřazené k dané klávese. Snaha byla vyjít z potisků písmen na jednotlivých klávesách, bohužel na klávese *7* chybí písmenko *Q*. To způsobuje posun písmen na všech následujících klávesách o jedno. Ve výsledku písmena začínají na klávese *2*, která generuje znaky **2ABC** a končí na klávese *0* kombinací **0YZ**.

Některým zbývajícím klávesám byly přiřazeny speciální funkce. Pro tečku a mezeru lze využít klávesy **#** a *****. Pro spuštění šifrování/dešifrování zapsaného textu slouží klávesa **A**. Pokud uživatel udělá v textu chybu, je možné smazat poslední písmeno klávesou **B**, případně smazat celý text klávesou **C**. Zbývající klávesy zůstávají nevyužity.

Pro nastavení rotorů a propojovací desky je nutné využít terminál. Ten zpracovává dva uživatelské příkazy, a to příkaz **ROTORS** a **PLUGBOARD**. Syntaxe těchto příkazů je následující:

1.1 ROTORS

Konfigurace rotorů:

```
ROTORS ID STATE ID STATE ID STATE
```

ID - identifikační číslo rotoru. Aktuální implementace obsahuje tři rotory s ID 1 - 3.
STATE - počáteční stav rotoru (0 - 25)

1.2 PLUGBOARD

Konfigurace propojovací desky:

```
PLUGBOARD AB CD EF ...
```

Jednotlivé kombinace musí obsahovat různá písmena a nesmí obsahovat již použitá písmena. Tato implementace podporuje maximálně 10 takových kombinací.

2 Implementace

Implementace je rozdělena na několik samostatně fungujících komponent, stejně jako u původního stroje.

2.1 Rotory

Rotory jsou válce, které slouží pro substituci jednotlivých znaků vstupního textu. Uvnitř válce jsou vedeny obvody, které konkrétní vstup připojí na určitý výstup. Tyto obvody byly neměnitelné, takže rotor pokaždé prováděl stejnou permutaci. Tato permutace je v programu implemetována pomocí jednoduchého pole znaků, které je uloženo ve struktuře představující celý rotor.

Další vlastností rotorů bylo jejich natočení. Tento stav ovlivňoval výsledek šifrování a měnil se po každém stisku klávesy na klávesnici stroje (platí pouze pro první rotor, změna stavu následujících rotorů je závislá na jejich další vlastnosti, viz dále). Každý rotor měl celkově 26 stavů (každé písmeno abecedy určovalo jeden stav rotoru). Stav je další součástí datové struktury rotoru.

Poslední součástí rotorů byl tzv. *carry notch*. Jedná se o zub, který při pootočení aktuální rotoru pootočí i rotor následující. I tato informace je uložena v datové struktuře rotoru.

[1] https://www.codesandciphers.org.uk/enigma/rotorspec.htm

2.2 Reflektor

Refletor je komponenta, která je vložena za poslední rotor a vede jeho výstup na určitý jeho vstup. Propojení uvnitř reflektoru je neměnné, stejně jako v případě rotorů. Reflektor je v programu implementován jako jednoduché pole znaků.

2.3 Propojovací deska

Propojovací deska je umístěna na čele stroje a jedná se o jednoduchou substituci vstupních i výstupních znaků za jiné. Tato substituce byla provedena kabelem, kterým byla jednotlivá písmena propojena a narozdíl od rotorů a reflektorů byla měnitelná uživatelem. I tato komponenta je implementována jako pole znaků.

Po implementaci všech potřebných komponent je nutné zajistit jejich správné propojení a operaci. Uživatel nejdříve napíše zprávu, která se zobrazí na LCD. Jakmile je se zprávou spokojen, stiskne klávesu **A**, která spustí proces šifrování či dešifrování, který probíhá následovně: každý znak je veden do propojovací desky, kde proběhne substituce. Její výsledek proveden přes všechny rotory, kde proběhnou patřičné substituce a posuny rotorů, směrem do reflektoru. Ten vstupní znak pomocí substituce zamění za jiný, který je předán na vstup posledního rotoru, kde se v této fázi provádí inverzní permutace. Pro provedení substitucí ve všech rotorech v obráceném pořadí je znak veden zpět do propojovací desky, jejíž vystup je uložen na patřičné místo vstupního řetězce. Po zpracování všech znaků je vstup na LCD nahrazen výsledným řetězcem.

3 Příklady

3.1 Příklad 1

Rotory: default (1 0 2 0 3 0)
Prop. deska: default (bez substitucí)
Vstup: HELLO WORLD.
Výstup: QHHLQ RMQUQ.

3.2 Příklad 2

Rotory: default (1 0 2 0 3 0)
Prop. deska: default (bez substitucí)
Vstup: QHHLQ RMQUQ.
Výstup: HELLO WORLD.

3.3 Příklad 3

Rotory: 1 15 2 10 3 11
Prop. deska: default (bez substitucí)
Vstup: SBYBZOD MVLAGW
Výstup: CTHULHU FHTAGN

3.4 Příklad 4

Rotory: 1 15 2 10 3 11
Prop. deska: FZ AD IM NS GH
Vstup: WIL ROH 2016
Výstup: VUT FIT 2016

3.5 Příklad 5

Rotory: 2 22 1 13 3 2
Prop. deska: FZ AD IM NS GH

Vstup: VLYG. HW. AEOASMV.
Výstup: THIS. IS. AWESOME.

3.6 Příklad 6

Rotory: 3 12 1 18 2 25
Prop. deska: AD BE CF LG MP
Vstup: KXRBIJOH WISKYZWY XEUAYM
Výstup: BENJAMIN FRANKLIN PIERCE

3.7 Příklad 7

Rotory: 1 25 2 25 3 25
Prop. deska: AB CD EF GH IJ
Vstup: UTDEG KEXXNJT
Výstup: GHOST BRIGADE

3.8 Příklad 8

Rotory: 1 25 1 25 1 25
Prop. deska: AB CD EF GH IJ
Vstup: JOPAH LPKUR
Výstup: AAAAA BBBBB

3.9 Příklad 9

Rotory: 2 25 1 25 1 25
Prop. deska: AB CD EF GH IJ
Vstup: AAAAA BBBBB
Výstup: GOLVM EJNQB

3.10 Příklad 10

Rotory: 2 25 1 25 1 25
Prop. deska: AB CD EF GH IJ
Vstup: GOLVM EJNQB
Výstup: AAAAA BBBBB

4 Závěr

Výsledkem této práce je funkční implementace stroje Enigma. S příhlédnutím na zadání byly splněny všechny požadavky.