# Vysoké Učení Technické v Brně

Fakulta informačních technologií


## Dokumentace k projektu do předmětu IMP

MSP430: Enigma

13. prosince 2016

Autor: Petr Flajšingr, xflajs00@stud.fit.vutbr.cz

# Úvod

Tato dokumentace obsahuje popis zadání projektu, implementace a funkčnosti.

Úkolem bylo vytvořit aplikaci fungující stejně jako šifrovací stroj Enigma, který byl využíván za druhé světové války. Projekt byl implementován podle „komerční Enigmy" vynalezené v roce 1924. Tato verze obsahuje takzvaný plugboard, který slouží k jednoduché záměně dvou znaků. Další částí jsou tři rotory, jejichž konfigurace je zobrazená níže v tabulce. Poté, co signál projde rotory, je vrácen zpět do rotorů reflektorem, který opět provádí substituci šifrovaného znaku. Nakonec signál opět projde plugboardem a zobrazí se zašifrovaný znak.

Rotory při zašifrování každého znaku mění svoji pozici a tím je zajištěno, že substituce znaků není vždy stejná.

| Rotor | Konfigurace |
|---|---|
| I | DMTWSILRUYQNKFEJCAZBPGXOHV |
| II | HQZGPJTMOBLNCIFDYAWVEUSRKX |
| III | UQNTLSZFMREHDPXKIBVYGJCWOA |

# Popis ovládání

Ovládání aplikace je realizováno čistě pomocí klávesnice na FITkitu a výstup je zobrazován v terminálu připojeného počítače. Klávesa „1" zobrazí v terminálu nápovědu pro použití. Tlačítka „2" až „9" slouží k zadávání znaků anglické abecedy stejně tak, jak tomu bylo u tlačítkových mobilních telefonů a klávesa „#" pro zadání vybraného znaku.

Pokud byla použita neplatná kombinace tlačítek je uživateli zobrazena chybová hláška.

Další sekcí je nastavení rotorů. Tlačítka „A", „B" a „C" umožňují nastavení jednotlivých rotorů. Zadávání konfigurace poté probíhá stejně jako zadávání znaků. Pomocí klávesy „D" lze nastavit rotory do výchozí pozice – v našem případě AAA. Posledním příkazem je zobrazení aktuální konfigurace rotoru. Toto je prováděno pomocí klávesy „*".

# Implementace

Pro rotory je využito pole hodnot simulující reálný rotor. Pro orientaci v konfiguraci rotoru jsou využity pomocné proměnné, ve kterých je uložen „offset" každého rotoru. Stejným způsobem je řešen i plugboard a reflector.

Pro práci s klávesnicí a LCD FITkitu jsem využil předem poskytnuté aplikace v SVN FITkitu.

## Ukázka šifrování

| Vstupní data | Šifrovaná data | Konfigurace rotorů |
|---|---|---|
| AAAAAAAAAA | PVQNXINSDB | GGG |
| ABCDEFGHIJ | PLKYMGWQXV | GGG |
| PVQNXINSDB | AAAAAAAAAA | GGG |
| LETADLOABC | YPFKRXRSRQ | ABC |
| RICHWOODGU | DYOYERRUKI | ABC |
| IBANEZROCK | CMEZWBOCSN | ABC |
| NESCAFEFTW | MIUXMTSVGC | ZZZ |
| SMETANOVYJ | XXQRRMSQFLO | ZZZ |
| DEKWOODPEN | CICBTBZZUL | ZZZ |
| ENIGMACOOL | CEXODOKIQO | FSJ |

## Závěr

Nedostatkem této implementace je využití cyklů pro procházení rotorů při návratu signálu z reflectoru. Původní plán byl vytvořit pole zvlášť pro průchod zpět, po hodinách útrap jsem od toho bohužel upustil.

Bylo by poměrně jednoduché rozšířit tuto implementaci o další rotory, případně implementovat možnost výměny rotorů nebo i nastavování plugboardu. Ovšem vzhledem k náročnosti těchto věcí mi připadalo zbytečné něco takového přidávat.

# Zdroje

Enigma rotor details. In: Wikipedia: the free encyclopedia [online]. St. Petersburg (Florida): Wikipedia Foundation, 11. 12. 2006, last modified on 10. 8. 2016 [cit. 2016-12-13]. Dostupné z: https://en.wikipedia.org/wiki/Enigma_rotor_details