VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

IMP – Mikroprocesorové a vestavěné systémy

M – MSP430-FitKit2: Šifrovací zařízení

Radek Duchoň 22. 12. 2019

1. Popis aplikace

Fitkit 2.0 s touto aplikací slouží jako jednoduché šifrovací zařízení. Konkrétně může šifrovat a dešifrovat zprávy pomocí Caesarovy šifry, pro kterou se nastavuje číselný posun v abecedě. Po spuštění se nejdříve vypíše nápověda oznamující základní ovládání aplikace. Po přečtení nápovědy (ke které se lze i vracet) uživatel může zadat číselný posun pro dekryptování/kryptování zprávy a následně samotnou zprávu a tu de/zašifrovat.

2. Popis ovládání

Jak uvádí na počátku programu nápověda, každé tlačítko má svůj význam, dle toho nejsou vždy všechna použitelná.

- A – Tlačítko dostalo význam „dále“ (next), pokud je to tedy možné, program přechází po stisku tohoto tlačítka do další části. V případě, že jsme již na zašifrované/dešifrované zprávě, jako bonus se stiskem inkrementuje šifrovací hodnotu o jedničku.
- B – Tomuto tlačítku byla přisouzena funkce „zpět“ (back), z libovolné části programu je tak možné vrátit se do dřívějších částí a upravit parametry, nebo se pročíst znovu nápovědu.
- C – Toto tlačítko funguje jako „shift“, po napsání písmene jej lze zvětšit nebo zmenšit stiskem tohoto tlačítka.
- D – Značí „smazat“ (delete), stiskem se umazává právě označení (uživatelem napsaný) znak.
- 1 – Po vyzvání k výběru zvolí šifrování zprávy
- 2 – Po vyzvání k výběru zvolí dešifrování zprávy
- 0-9 – Slouží pro zadávání znaků, v módu zadávání šifrovacího čísla se jedná o čísla, při psaní samotné šifry se pak zadávají znaky podobně jako na telefonu
- # – Slouží pro posun v napsaných znacích zpět. (Při zobrazování zprávy pak rolluje zprávu na displeji a umožňuje tak zobrazovat až 40 znakové zprávy.)
- * – Slouží pro posun v napsaných znacích dopředu. V módu psaní zprávy je nutné toto tlačítko používat k posunu na další znak. (Při zobrazování zprávy pak rolluje zprávu na displeji a umožňuje tak zobrazovat až 40 znakové zprávy.)

3. Příklady zpráv

Klíč (posunutí) je o tolik, na kolikátém řádku daná zpráva je:

```
1. Preji prijemne stravene svatky.  -> Qsfkj qsjkfnof tusbwfof twbulz.
2. Stastne a vesele Vanoce!         -> Uvcuvog c xgugng Xcpqeg!
3. Stastny Novy rok!                -> Vwdvwqb Qryb urn!
4. Vanoce jsou obdobi klidu a miru. -> Zersgi nwsy sfhsfm opmhy e qmvy.
5. ... A nebo snad ne?              -> ... F sjgt xsfi sj?
6. Blizi se zkousky... :(           -> Hrofo yk fquayqe... :(
7. Bakalarce se nestiham venovat :( -> Ihrhshyjl zl ulzapoht cluvcha :(
8. Toto je predposledni projekt!    -> Bwbw rm xzmlxwatmlvq xzwrmsb!
9. Brzy uz bude konec :)            -> Kaih di kdmn txwnl :)
10.Uz jen pul roku... :)            -> Ej tox zev byue... :)
```

4. Popis řešení

Klíčové prvky:

- lcd_cursor_addr – Externí globální proměnná, která říká, kde se právě nachází kursor, využívaná pro snadné a efektivnější přemisťování na jiné pozice.
- Makra – Lze rozdělit na 2 typy – pro přehlednost, jako například next(c), nebo pro zjednodušení psaní, kdy makro sdružuje několik instrukcí, pro bezpečnost obalených ve konstrukci do {} while (0). Často pracují s výše zmíněnou proměnnou (například pro nastavení pozice na druhý řádek apod.)
- goto – v tomto projektu pracuji relativně hodně (vůči jeho velikosti) s goto, a to protože mi to takto přišlo nejen programátorsky jednodušší, ale hlavně přehlednější, než aby bylo vše zabaleno v několikanásobném nekonečném cyklu, ve chvíli kdy jsem chtěl, aby se šlo vracet k předchozím částem programu a i nápovědě na začátek. Díky tomuto řešení by nebylo teoreticky vůbec těžké přidat další mezikroky, například pro volbu z více šifer, kdy by zpravidla mělo stačit přidat nové návěští s novou funkcinalitou a upravit jedno (následující) goto zpět.

5. Závěr

Aplikace dle mého názoru splňuje zadání a přináší i něco navíc. (Například možnost posouvat šifrovací klíč jednoduše pomocí kláves ‚A' a ‚C'.) Lze využít i scrollování displeje a mít tak zprávy až o čtyřiceti znacích. 40 znaků je však také implementační limit tohoto řešení, pokud by měly být zprávy najednou delší, bylo by nutné navrhnout řešení tohoto programu jinak.