Návrh počítačových systémů 2025 - projekt 2

Název: Souhláskově modulovaná samohlásková šifra na architektuře MIPS64
Bodové hodnocení: max. 10b
Datum odevzdání: nejpozději 12.12.2025
Dotazy: → Marcela Zachariášová, L339, zachariasova@fit.vut.cz

Cíl projektu: porozumět principům zřetězeného zpracování instrukcí v procesorech pomocí vizualizace zřetězené linky procesoru MIPS64.

Zadání:

V jazyku symbolických instrukcí MIPS64 a s využitím simulátoru EduMIPS64 napište program realizující **souhláskově modulovanou samohláskovou šifru** podle následující specifikace:

1. **Šifrovány jsou pouze samohlásky** (a, e, i, o, u, y). Souhlásky zůstávají beze změny.
2. **Každá samohláska je šifrována dynamickým klíčem**, který se odvozuje z **pozice předchozí souhlásky ve správě od začátku abecedy.**
   Například: pokud je před samohláskou „**a**" souhláska „**d**", použije se klíč odpovídající číslu **4** (protože „d" je čtvrté písmeno abecedy).
   Tento klíč určuje, o kolik pozic se samohláska posune v abecedě: (**a** → b → c → d → **e**).
3. Pokud samohlásce nepředchází žádná souhláska na začátku slova, uvažujeme souhlásku „z". Pro dvě po sobě následující samohlásky se použije stejný klíč daný předchozí souhláskou.
4. Posuvy jsou cyklické, tj. vychází-li zašifrovaný znak před písmeno „a" nebo za písmeno „z", uvažují se znaky z opačného konce abecedy.

Uvažujte zprávu tvořenou výhradně malými písmeny anglické abecedy a-z reprezentující vaše **jméno a příjmení** (bez mezer, bez diakritiky či jiných nepísmenných znaků).

Příklad: zpráva: marcelazachariasova
Postup šifrování:

```
zpráva: m  a r c  e l  a z  a c h  a r  i  a s  o v  a
klíč:      m     c    l    z     h    r  r    s    v
posuv:    +13   +3   +12  +26   +8   +18+18  +19  +22
       ---------------------------------------------
        m  n r c  h l  m z  a c h  i r  a  s s  h v  w

            mnrchlmzachirasshvw ←  zašifrovaný text
```

Stažení a používání EduMIPS64

Stáhněte si simulátor EduMIPS64 (https://edumips.org/): doporučuji z git-webu k poslední verzi stáhnout binárku .jar (pro win instalátor .msi) a dokumentaci v pdf.

Seznamte se s obsluhou simulátoru. Začněte např. výpisem nápovědy:

java -jar edumips64-1.3.0.jar --help

Podrobná dokumentace včetně popisu instrukční sady je součástí aplikace v menu Help → Manual… Samostatně je instrukční sada MIPS64 popsána např zde:

https://edumips64.readthedocs.io/en/latest/instructions.html

Do stejného adresáře jako .jar soubor zkopírujte vzorový soubor hello.s a ověření funkčnosti simulátoru proveďte spuštěním:

java -jar edumips64-1.3.0.jar -f hello.s

Takto nahraný program lze spustit (F4) nebo krokovat (F7). Měl by vypsat uvítací řetězec Hello world! Stav simulace lze kdykoli resetovat do výchozího stavu (jako po nahrání programu) stiskem Ctrl-R.

Pokyny k řešení a odevzdání

Na prvním řádku doplňte **bez diakritik**y vaše jméno, příjmení a login. **Stejné jméno a příjmení se očekává též v proměnné msg!**

Uvítací řetězec uvozený návěštím **msg:** nahraďte vaším jménem a příjmením **bez mezer, bez diakritiky**. Jako šifrovací klíč pro samohlásky uvažujte pozici předchozí souhlásky od začátku abecedy. Ascii kódy samohlásek napevno vhodným způsobem reprezentujte v programu, abyste s nimi mohli jednoduše počítat. Program musí umět dle popsaného algoritmu šifrovat libovolný písmenný řetězec, jeho max. délku předpokládejte 30 znaků (bez ukončující 0), jak je vyhrazeno za návěštím cipher.

Návěštím **cipher:** je uvozeno vyhrazené místo pro zašifrovaný text. Sem zapisujte zašifrované znaky. **Neměňte alokovanou velikost.**

Návěští **param_sys5:** alokuje prostor pro předání argumentu "funkci" uvozenou návěštím **print_string:** pro výpis textového řetězce. Výpis je realizován systémovým voláním syscall 5. Voláním print_string nakonec vypište zašifrovaný text. Pro správnou funkci výpisu musí být řetězec ukončen hodnotou 0 (podobně jako řetězec v C).

Za návěštím **main:** je minimální vzorový kód pro výpis uvítacího řetězce (vizte komentář v kódu). Sem zapište namísto tohoto kódu Vaše řešení. Po dokončení **přejmenujte soubor hello.s na xlogin00.s (s vaším loginem!)** a samotný tento soubor odevzdejte k zadání Projektu 2 INP v IS.

Upozornění k hodnocení

Pečlivě si ověřte, co odevzdáváte. Nepřeložitelná, nespustitelná nebo havarující řešení budou hodnocena 0 body. **Vyučující zásadně neprovádí změny v odevzdaných souborech,** ať jsou jakkoli drobné! Zjištěné **plagiáty budou též za 0b,** navíc s případným postihem a ostudou od Disciplinární komise FIT!