Návrh počítačových systémů 2024 - projekt 2

Název: Vigenèrova šifra na architektuře MIPS64
Bodové hodnocení: max. 10b
Datum odevzdání: nejpozději 1.12.2024
Dotazy: → Michal Bidlo, L330, bidlo@fit.vut.cz, přehled předpokládané dostupnosti vyučujícího s možností rezervace termínu konzultace na https://ehw.fit.vutbr.cz/rezervace/bidlom.

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 mírně pozměněný algoritmus **Vigenèrovy šifry** podle následující specifikace. Jde o proudovou substituční šifru, šifrování spočívá v nahrazování každého písmene zprávy jiným písmenem, které je v abecedě posunuto dle příslušných písmen šifrovacího klíče: ‘a’ posouvá o jedno písmeno, ‘b’ o dvě písmena, ‘c’ o tři atd. Uvažujme střídavý posuv vpřed a vzad v abecedě s každým písmenem klíče. Šifrování bude vždy zahájeno posuvem vpřed. 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). Šifrovací klíč bude tvořen prvními třemi písmeny vašeho příjmení bez diakritiky a bude se periodicky opakovat přes jednotlivé znaky zprávy.

Příklad: zpráva: michalbidlo, klíč: bid. Postup šifrování:

```
zpráva: m  i  c  h  a  l  b  i  d  l  o
klíč:   b  i  d  b  i  d  b  i  d  b  i
posuv: +2 -9 +4 -2 +9 -4 +2 -9 +4 -2 +9
       --------------------------------
        o  z  g  f  j  h  d  z  h  j  x   ←  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 možná 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 uvažujte první tři znaky vašeho příjmení bez diakritiky. Jejich ascii kódy napevno vhodným způsobem reprezentujte v programu, abyste s nimi mohli dále 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 reaizován 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 vozrový 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 ve STUDISu.

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!