Návrh počítačových systémů 2022 - projekt 2

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

Cíl projektu: porozumět základním principům a vybraným problémům zřetězeného zpracování instrukcí v procesorech

Zadání:

V jazyku symbolických instrukcí MIPS64 a s využitím simulátoru EduMIPS64 napište program realizující lehce modifikovaný, zjednodušený algoritmus **Vernamovy šifry**. Vernamova šifra patří do kategorie substitučních šifer a její princip pro potřeby tohoto projektu bude spočívat v nahrazování každého písmene zprávy jiným písmenem, které je v abecedě posunuto o hodnotu danou příslušným písmenem šifrovacího klíče. Uvažujte zprávu tvořenou výhradně malými písmeny anglické abecedy a-z a číslicemi 0-9. Šifrovací klíč o pevné délce dvou znaků bude tvořen písmeny anglické abecedy a-z, které se periodicky opakují přes jednotlivé znaky zprávy. Znaky budou pro potřeby šifrování reprezentovány svými ASCII kódy. Šifrování bude probíhat tak, že je zpráva čtena znak po znaku zleva doprava, první znak klíče posouvá přečtený znak vpřed, druhý znak klíče posouvá znak vzad. **Pokud je přečtena číslice, je šifrování ukončeno** a jako výsledek je vypsán zašifrovaný text. Posouvání znaků je cyklické, tj. vychází-li posuv před písmeno ‘a’ nebo za písmeno ‘z’, pokračuje se z opačného konce abecedy – vizte příklad níže. **Jiné znaky než a-z, 0-9 se na vstupu nepředpokládají** (nemusíte je vzlášť ošetřovat). Lze tak např. určit, že pokud má načtený znak ASCII hodnotu menší než 97 (tj. je před písmenem ‘a’), jedná se o číslici (číslice jsou v ASCII tabulce před písmeny). **Váš program musí být schopen dle výše uvedených pravidel korektně šifrovat řetězce sestávající z libovolné kombinace uvedených znaků.**

Příklad: zpráva: xbidlo01, klíč: bi (‘b’ posouvá o 2 znaky vpřed, ‘i’ posouvá o 9 znaků vzad). Postup šifrování:

```
zpráva: x  b  i  d  l  o  0  1
klíč:    b  i  b  i  b  i
posuv: +2 -9 +2 -9 +2 -9
       ----------------------
        z  s  k  u  n  f  ←  zašifrovaný text
```

Pokyny k řešení

1. Stáhněte si simulátor EduMIPS64 (https://edumips.org/) - nejlépe ve formátu jar. Funguje na různých OS, jen je nutné mít nainstalovanou Javu v požadované minimální verzi.

2. Seznamte se se základy obsluhy simulátoru dle následujících pokynů. Doporučuji nejprve vypsat nápovědu spuštěním příkazu:

java -jar edumips64-1.2.10.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 edumips64-1.2.10.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.

3. Seznamte se se strukturou vzorového programu:

Uvítací řetězec uvozený návěštím **login:** nahraďte vaším loginem. Jako šifrovací klíč uvažujte první dva znaky vašeho příjmení (konkrétně jsou to ty ve vašem loginu za ‘x’). **Jejich ascii kódy napevno vhodným způsobem reprezentujte v programu, abyste s nimi mohli dále počítat.**

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 login. 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).

4. Vaše řešení zapište namísto kódu za návěštím **main**. **Ze souboru registry.txt si podle loginu zjistěte**, které registry můžete používat. **Na registry se odkazujte výhradně pomocí symboliky ‘r’** (tedy ne pomocí alias $). **Nedodržení těchto pravidel může vést ke ztrátě bodů!** Po dokončení **přejmenujte soubor hello.s na xlogin00.s (váš login)** a takto odevzdejte k zadání Projektu 2 INP ve STUDISu (**bez zipování!**).

Upozornění k hodnocení

Bude-li řešení nepřeložitelné nebo pokud program skončí chybou, bude hodnoceno 0 body, přičemž bude **JEDNOU** umožněno zaslání opravené verze a komentáře k opravě mailem do stanoveného data **s možnou bodovou ztrátou úměrnou závažnosti opravy. Vyučující zásadně neprovádí jakékoli změny v odevzdaných souborech. Opakovaně nefunkční řešení budou hodnocena 0 body.** Stejně tak zjištěné **plagiáty budou za 0b**, navíc s případným postihem a ostudou od Disciplinární komise FIT!