Návrh počítačových systémů 2021 - projekt 2

Název: Vernamova šifra – výpočet na zřetězené architektuře DLX
Datum odevzdání, bodové hodnocení: vizte termín Projekt 2 v IS FIT
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

Zadání:

V jazyku symbolických instrukcí procesorové architektury DLX a s využitím simulátoru OpenDLX tohoto procesoru 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 na vstupu pro jednoduchost neuvažujte (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, protože jiné znaky se neočekávají (číslice jsou v ASCII tabulce před písmeny). **Váš program musí být schopen dle výše uvedených pravidel korektně šifrovat řetězce sestávající z libovolné kombinace malých písmen anglické abecedy a číslic.**

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 OpenDLX. Funguje na různých OS, jen je nutné mít nainstalovanou Javu (vizte popis v dokumentaci). https://sourceforge.net/projects/opendlx/

2. Spusťte simulátor DLX a v něm otevřte (Ctrl+o) soubor vernam.s. Zobrazí se okno “coding frame” s kostrou projektu. Stiskněte tlačítko “assemble” – proběhne překlad a zobrazí se další okna (obsahy registrů, paměti atd.). Stiskněte F5 (Run program), čímž dojde k vykonání programu a měli byste vidět výpis uvítací hlášky. Stiskněte Enter (close), zobrazí se hláška “simulation finished”. Tím je ověřena funkce simulátoru, pokračujte dalšími kroky.

3. V souboru vernam.s vyplňte záhlaví na druhém řádku a nahraďte uvítací řetězec u návěští login vaším loginem – s tím budete projekt odevzdávat. Jako šifrovací klíč uvažujte první dva znaky vašeho příjmení (konkrétně jsou to ty ve vašem loginu za ‘x’).

4. **Ze souboru registry.txt si podle loginu zjistěte**, které registry můžete ve svém řešení používat. Každý má unikátní, dostatečně bohatou množinu registrů. **Použití jiných registrů není dovoleno.** Porušení tohoto pravidla může vést ke ztrátě bodů!

5. Za návěštím cipher je vyhrazeno neinicializované místo pro zašifrovaný text. Sem zapisujte zašifrované znaky. Za návěštím end je připraven kód pro výpis uvítacího textu pomocí systémového volání (trap), který změnte na výpis zašifrovaného textu. Pro správnou funkci výpisu musí být řetězec ukončen hodnotou 0. **Řiďte se komentáři v textu a vaše řešení též přiměřeně komentujte.**

6. Za návěští main zapište vaše řešení. Po dokončení **soubor vernam.s přejmenujte na váš login** (se zachováním přípony .s) a odevzdejte do IS FIT (**bez zipování nebo jiných příloh**).

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 případným drsným postihem a ostudou od Disciplinární komise FIT!