Návrh počítačových systémů 2020 - projekt 1

Název: Vigenèrova šifra
Datum odevzdání: vizte termín Projekt 1 v IS FIT
Počet bodů: max. 15
Dotazy: vizte kontakt na https://ehw.fit.vutbr.cz/rezervace/bidlom s možností rezervace termínu konzultace osobně na FIT nebo online.

Zadání:

V jazyce VHDL popište, programem Xilinx Isim odsimulujte a do binárního řetězce pro FPGA syntetizujte obvod realizující lehce modifikovaný algoritmus **Vigenèrovy šifry**. Vigenèrova šifra patří do kategorie substitučních šifer a její princip pro potřeby tohoto projektu bude spočívat v nahrazování každého znaku zprávy znakem, který je v abecedě posunut o hodnotu danou příslušným znakem šifrovacího klíče. Uvažujte zprávu tvořenou velkými písmeny anglické abecedy A-Z (tj. pouze znaky bez diakritiky, CH je bráno jako dva samostatné znaky) a číslicemi 0-9. Šifrovací klíč o pevné délce dvou znaků bude tvořen písmeny anglické abecedy A-Z a periodicky se opakuje přes všechny znaky zprávy. Znaky budou pro potřeby šifrování reprezentovány svými ASCII kódy. Šifrování bude probíhat tak, že první znak klíče posouvá znak zprávy vpřed, druhý znak klíče posouvá znak zprávy vzad, číslice jsou nahrazovány znakem #. Pokud vychází posuv před písmeno A nebo za písmeno Z, uvažuje se cyklicky z opačného konce abecedy – vizte příklad.

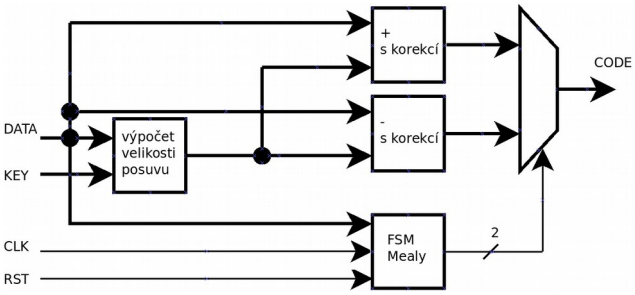
Příklad: zpráva XBIDLO01, klíč BI (B posouvá o 2 znaky vpřed, I posouvá o 9 znaků vzad). Postup šifrování:

```
zpráva: X  B  I  D  L  O  0  1
klíč:   B  I  B  I  B  I  B  I
posuv: +2 -9 +2 -9 +2 -9 +2 -9
       ------------------------
        Z  S  K  U  N  F  #  #  ← zašifrovaný text
```

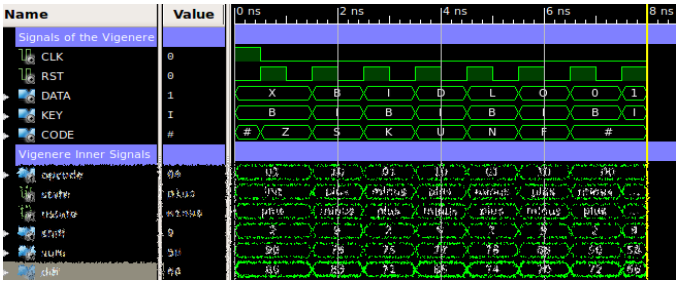
Pokyny k vypracování:

- Vytvořte **bez chyb a varování syntetizovatelný popis** obvodu (nápověda k řešení je na obr. 1) s **Mealyho** variantou FSM (navrhněte jeho efektivní podobu). Řešení doplňte do souboru **fpga/vigenere.vhd**.
- Soubor **fpga/sim/tb.vhd** obsahuje testbench, v něm si upravte symboly zprávy a klíče dle vašeho loginu a prvních dvou znaků příjmení bez diakritiky. Příklad: pro příjmení Šimek bude šifrovací klíč SI.
- Soubor **fpga/sim/isim.tcl** obsahuje skript pro pohodlné zobrazení simulačního diagramu v aplikaci Xilinx Isim (příklad diagramu je na obr. 2). Spodní část diagramu je záměrně rozostřena, je předmětem řešení projektu. Dodržte pojmenování signálů rozhraní obvodu z obr. 1, vnitřní signály si pojmenujte sami, doplňte jejich identifikátory do souboru **isim.tcl** a zahrňte je takto všechny do simulačního diagramu pod oddělovač “Vigenere Inner Signals”. **Nekomplikujte řešení zbytečnými signály**, snažte se o jednoduchost a efektivitu.

- Při aktivním signálu *reset* generujte na výstupu CODE znak #.
- V každém hodinovém taktu se bude zpracovávat jeden znak.
- Simulaci vyvoláte zadáním příkazu *make isim* (ve win *gmake isim*) v hlavním adresáři projektu nakopírovaného do stromu projektů k FITkitu (po vygenerování překladových souborů příkazem fcmake).
- Inspirujte se příklady z přednášky a cvičení, dodržujte zásady psaní syntetizovatelného VHDL – vizte též popis na http://merlin.fit.vutbr.cz/FITkit/docs/navody/synth_templates.html.



Obrázek 1: schéma obvodu (tlusté spoje jsou na 8 bitů)



Obrázek 2: příklad simulace

Odevzdání, hodnocení

Doplněné řešení odevzdejte do IS v jediném archivu .zip nebo .tar.gz se **stejnou strukturou, jak jste si jej stáhli (závisí na tom automatizovaný překlad pro hodnocení). Archiv i adresář v něm pojmenujte vaším loginem.**

Jednou z podmínek pro získání plného počtu bodů je bezchybná kompilace VHDL kódu i syntéza konfigurace pro FPGA příkazem *make* (ve win *gmake*), tj. **žádný warning nebo error!**

Zkontrolujte si, zda opravdu odevzdáváte všechny správné soubory v archivu s danou strukturou. Bude-li projekt z jakéhokoliv důvodu nepřeložitelný, bude **JEDNOU** umožněno zaslání opravené verze a komentáře k opravě mailem do stanoveného data **s možnou bodovou ztrátou úměrnou závažnosti opravy. Vyučující zásadně neprovádí jakékoliv změny v odevzdaných souborech. Opakovaně nepřeložitelná řešení budou hodnocena 0 body,** stejně tak jako v případě zjištěného **plagiátorství - v takovém případě navíc s případným postihem dle platného Disciplinárního řádu FIT VUT v Brně.**