Slovenská technická univerzita v Bratislave

Fakulta elektrotechniky a informatiky

Katedra informatiky a výpočtovej techniky

Posudok dokumentácie

Implementácia blokového šifrátora pomocou PLD

tímu č.11 od tímu č.12

tím č. 12:

Bc. Martin Prokša

Bc. Viliam Otepka

Bc. Ivan Varga

Bc. Martin Zeman

vedúci projektu: doc. Ing. Ladislav Hudec, CSC

šk. rok: 2002/2003

1 Úvod

Posudzovaný projekt sa zaoberá implementáciou blokového šifrátora do PLD obvodu. Projekt je rozdelený na dve časti. Úlohou prvej časti je vytvoriť interaktívnu prezentáciu blokovej šifry IDEA, pričom v druhej časti sa šifra implementuje do zvoleného PLD obvodu.

Cieľom tohto dokumentu je posúdiť prvú časť dokumentácie tímu č.11 v zložení:

- Bc. Radovan FRAŇO
- Bc. Peter JŮZL
- Bc. Rastislav LAUKO
- Bc. Michal LEHOTSKÝ
- Bc. Róbert ŠEVČÍK

Na hodnotení sa podieľali členovia tímu č.12, menovite:

- Bc. Ivan VARGA
- Bc. Martin PROKŠA

Hodnotená bola obsahová aj formálna stránka, celková zrozumiteľnosť, úplnosť a konzistentnosť doteraz vytvorenej dokumentácie.

2 Formálna stránka

Odovzdaný dokument obsahuje 25 strán textu dokumentácie projektu a 7 strán dokumentácie k riadeniu projektu. Dokumentácia ďalej obsahuje zápisnice zo stretnutí atď., pričom celá je uzatvorená v praktickom karisblokovom obale.

Dokument neobsahuje gramatické chyby. Vyskytli sa iba preklepy alebo zle nasádzané písmená čo však je chybou použitého textového programu a nie členov tímu. Výhrady máme iba k nepreloženým anglickým výrazom použitých v obr. 2.1 a obr. 2.2.

3 Zhodnotenie jednotlivých častí dokumentácie projektu po obsahovej stránke

3.1 Úvod

Kapitola má podľa osnov obsahovať stav projektu a ciele, dokumentáciu, ohraničenia a riešiteľský kolektív. Tím dodržal tieto predpísané body, čím boli podmienky kladené na túto kapitolu splnené. Výhrady máme iba k zmene osoby z pohľadu ktorej je dokument napísaný. Táto zmena sa vyskytuje v časti 1.3. Riešiteľský kolektív.

3.2 Analýza

Analýza taktiež spĺňa všetky ciele. Popisuje činnosť šifrovacieho algoritmu IDEA názorným obrázkom (obr. 2.1) a slovným popisom. Slovný popis je vcelku dobre napísaný ale zbytočne podrobný a pre laika neprehľadný. Uprednostnili by sme jednoduchší popis pomocou obrázku a pre lepšie oboznámenie práce algoritmu prenecháme interaktívnej prezentácii. Táto časť dokumentu obsahuje aj analýzu PLD obvodov čo je náplň až druhej polovice projektu v letnom semestri, avšak uvedená analýza je veľmi dobre rozpracovaná. Dokumentácia obsahuje aj prehľad vlastností jednotlivých PLD obvodov ako aj prehľad jednotlivých implementácií šifrovacieho algoritmu softvérovými alebo hardvérovými prostriedkami.

3.3 Špecifikácia

Podmienky kladené na túto kapitolu boli splnené. Vyskytla sa iba maličká chyba, kedy bola nesprávne uvedená veľkosť kľúča (64 bitov) a veľkosť šifrovaného textu (128 bitov) konkrétne na strane 14. Ide však iba o preklep,

pretože ostatné zmienky o veľkosti kľúčov sú správne.

Trochu nás zarazila skutočnosť, že konkurenčný tím neuvažuje o zaradení dešifrovania do interaktívnej prezentácie algoritmu IDEA. Sme toho názoru, že pre prezentáciu šifry je dôležité predstaviť aj algoritmus na dešifrovanie. Vzhľadom na to, že na dešifrovanie sa používa rovnaký algoritmus, jediné v čom sa dešifrovanie odlišuje je odlišný algoritmus výpočtu podkľúčov, by zaradenie dešifrovania neprinieslo veľké úpravy prezentácie.

3.4 Návrh

Návrh obsahuje všetky potrebné informácie. Riešiteľský tím sa zbytočne zaoberal vzhľadom web stránky venujúcej sa tímovému projektu. V návrhu sa mali zamerať na spracovanie iba interaktívnej prezentácie samotnej šifry ktorá je v dokumente stručne a vecne popísaná. Tím rozdelil celú prezentáciu na dve časti. Na interaktívnu časť v ktorej sa prezentujú výsledky šifrovania a výpočtovú v ktorej sa vyčíslia tieto výsledky. Na interaktívnu prezentáciu použili nástroj Macromedia FLASH ktorý obsahuje programovací jazyk schopný obsiahnuť algoritmus šifrovania. Týmto rozdelením sa zbytočne komplikuje celá prezentácia a zbytočne sa vyžaduje existencia podpory JAVA na hostiteľskom počítači.

Riešiteľský za v návrhu nezaoberal správou podkľúčov na dešifrovanie a ani matematickou operáciou potrebnou na výpočet dešifrovacích podkľúčov „Inverzným násobením“.

3.5 Riadenie Projektu

Výhrady ani zásadné pripomienky k riadeniu nemáme. Tím si zvolil dopracovanie web prezentácie v 12 týždni. Ak by splnili tento plán neostane im žiadny čas na otestovanie a prípadne opravenie zistených chýb.

4 Záver

Pri posudzovaní celej dokumentácie k produktu sme dospeli k názoru, že tím č.11 má problematiku pomerne dobre zvládnutú. Zásadné negatíva sme nezistili. Dokumentácia pôsobí kompaktným dojmom. Gramatické ani formálne chyby sa prakticky nevyskytujú. Po obsahovej stránke má dokumentácia niekoľko malých chýb ktoré sa v krátkom časovom horizonte dajú napraviť.

Jediná vážnejšia vec, čo by sme chceli recenzovanej práci vytknúť je nezoberanie sa dešifrovaním a to ani v interaktívnej prezentácie, kde by si zaradenie tohoto módu práce naozaj nevyžiadalo veľkú námahu. Dešifrovanie považujeme za dôležitú súčasť prezentácie, aby si používateľ mohol overiť výsledky, získané šifrovaním. Vzhľadom na tieto skutočnosti a ešte stále ostávajúci čas do odovzdania, by sme chceli tímu č. 11 navrhnúť, aby ešte zvážil zaradenie dešifrovania do konečnej prezentácie algoritmu IDEA.

Nakoniec by sme chceli upozorniť konkurenčný tím, aby nebral nami vypracovaný posudok ako príliš kritický a útočný, ale len ako posudok, odzrkadľujúci reálny stav riešenia projektu.