Posudek oponenta bakalářské práce

Student: Balvín David
Téma: Šifrování nad textovými zprávami pro Android (id 20391)
Oponent: Burget Radek, Ing., Ph.D., UIFS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

2. Splnění požadavků zadání **zadání splněno**

Zadání považuji za splněné bez výhrad.

3. Rozsah technické zprávy **je v obvyklém rozmezí**

Rozsah technické zprávy je v rozmezí obvyklém pro bakalářskou práci.

4. Prezentační úroveň předložené práce **74 b. (C)**

Technická zpráva je dobře strukturovaná a pokrývá jak teoretickou část sestávající zejména z rozboru relevantních kryptografických metod a souvisejících technologií, tak i praktickou část, která se soustředí na návrh a implementaci aplikace na platformě Android. Ve srovnání s teoretickou částí je praktická část zpracována poněkud stručně a největší prostor je věnován návrhu uživatelského rozhraní. Vlastnímu šifrování je oproti tomu věnováno mnohem méně prostoru a mnohé praktické aspekty nejsou v technické zprávě rozebrány. Také popis testování se soustředí pouze na uživatelské rozhraní aplikace.

5. Formální úprava technické zprávy **80 b. (B)**

Z formálního hlediska je technická zpráva poměrně pečlivě zpracována, nemám vážnější výhrady po jazykové ani typografické stránce.

6. Práce s literaturou **80 b. (B)**

Seznam použité literatury je poměrně rozsáhlý, zvolené zdroje jsou relevantní a pokrývají řešenou problematiku. Ojediněle lze narazit na chyby v údajích, např. zdroj [26]. Jednotlivé zdroje jsou v textu řádně citovány.

7. Realizační výstup **74 b. (C)**

Realizačním výstupem je aplikace pro mobilní telefony s operačním systémem Android, která umožňuje zasílání jak šifrovaných, tak nešifrovaných textových zpráv a jejich případné dešifrování při přijetí. Součástí je i jednoducý obecný nástroj pro šifrování textu. Aplikace není příliš rozsáhlá, nicméně požadavky zadání splňuje. Přesto mohl autor věnovat více pozornosti praktickým aspektům, jako např. efektivita použitého kódování, integrace s dalšími aplikacemi apod. Na druhou stranu student implementoval některá rozšíření oproti zadání, např. Huffmanovo kódování.

8. Využitelnost výsledků

Výsledná aplikace je použitelná pro základní zasílání šifrovaných textových zpráv a jejich dešifrováni.

9. Otázky k obhajobě

1. Jaké úpravy v návrhu, implementaci a volbě algoritmů by bylo nutné udělat, aby se minimalizoval objem přenášených dat?

10. Souhrnné hodnocení **75 b. dobře (C)**

Výsledkem práce pana Balvína je nepříliš rozsáhlá, nicméně plně funkční aplikace pro mobilní telefony a poměrně pečlivě zpracovaná technická zpráva, ke které mám jen některé, výše uvedené výhrady. Celkově proto hodnotím práci jako průměrnou a navruji hodnocení stupněm C.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 11. srpna 2017

.....
podpis