Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Milan Oulehla** **Oponent:** **Ing. Petr Hrůza, Ph.D.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Informační technologie**
Akademický rok: **2012/2013**

Téma diplomové práce: **Šifrování dat na mobilních zařízeních Android**

Hodnocení práce:

Cílem diplomové práce Bc. Milana OULEHLY na téma *„Šifrování dat na mobilních zařízeních Android"* bylo popsat charakteristiku současných technologií kryptografie pro mobilní platformu Android, specifikovat omezení a navrhnout kryptografickou aplikaci pro mobilní platformu Android.

Diplomová práce v teoretické části pojednává o historii šifrování a druzích symetrického a asymetrického šifrování. Pro jednotlivé typy šifrování jsou uvedeny praktické příklady, na kterých je prezentován celý postup šifrování a dešifrování. Dále jsou vysvětleny matematické základy útoku na RSA. V druhé části je uvedena charakteristika současných technologií kryptografie pro mobilní platformu Android. Teoretická část diplomové práce je zpracovaná na vysoké úrovni a mohla by sloužit studentům a zájemcům o oblast šifrování jako studijní materiál objasňující tuto problematiku.

Praktická část diplomové práce se věnuje omezením současných technologií kryptografie pro mobilní platformu Android. Následně je v práci navržena originální kryptografická aplikace pro mobilní platformu Android, která respektuje moderní požadavky ochrany dat. Aplikaci jsem prakticky odzkoušel a musím konstatovat, že je zcela funkční. Dále jsou definovány požadavky a podmínky přenosu šifrovaných souborů mezi mobilními zařízeními s operačním systémem Android. Velice kladně hodnotím podrobný popis vývoje aplikace doplněný názornými obrázky. V práci je také přehledně objasněna problematika GUI návrhu pomocí jazyka XML. Autor dále vytvořil vlastní návrh přenosu šifrovaných souborů mezi mobilními zařízeními s operačním systémem Android. Návrh využívá interaktivní spolupráce SSHD serveru s mobilními zařízeními.

Základní struktura diplomové práce je logická a jednotlivé kapitoly práce na sebe navazují. V závěru práce autor jednoznačně a srozumitelně shrnuje zjištěné poznatky. V diplomové práci autor uvádí adekvátní množství obrázků k objasnění popisované problematiky. Seznam literatury zahrnuje odpovídající množství relevantních zdrojů. Autor splnil zadaný cíl a práci je možné charakterizovat jako původní. Postup řešení, který autor zvolil, byl správný a logický v souladu se stanoveným tématem, cílem, omezujícími a výchozími podmínkami práce.

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Při obhajobě prosím o zodpovězení následujících otázek:

1. **Jsou možná nějaká další rozšíření návrhu aplikace?**

2. **Je možné přidat do návrhu aplikace další způsoby šifrování (například RSA)?**

Celkové hodnocení práce:
Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě".

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

V případě hodnocení stupněm „F – nedostatečně" uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 27.5.2013

Podpis oponenta diplomové práce