Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

# POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

**Student:** **Bc. Petr Žáček** **Oponent:** **Ing. Martin Spurný**

Studijní program: **Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Akademický rok: **2013/2014**

Téma diplomové práce: **Návrh nové symetrické šifry pro mobilní zařízení**

**Hodnocení práce:**

Cílem diplomové práce Bc. Petra ŽÁČKA na téma *„Návrh nové symetrické šifry pro mobilní zařízení“* bylo navrhnout blokovou symetrickou šifru a její implementací v programovacím jazyce Python verze 3.x. Analyzovat bezpečnost a rychlost navrženého symetrického algoritmu pro šifrování a jeho porovnání se známými symetrickými šifrovacími algoritmy DES, 3DES a AES. Dále vytvořit grafické uživatelské rozhraní pro použití navržené šifry k šifrování a dešifrování souborů a zhodnotit využitelnost navržené symetrické šifry pro mobilní zařízení.

Diplomová práce se v teoretické části práce zabývá základním popisem moderní symetrické kryptografie s nejznámějšími blokovými šiframi, rozborem jejich možností, strukturou a operacemi pro šifrování a dešifrování. Pro jednotlivé typy šifrování jsou uvedeny praktické příklady, na kterých je prezentován celý postup šifrování a dešifrování. Teoretická část diplomové práce je zpracována na velmi dobré úrovni, jasně a srozumitelně.

Praktická část diplomové práce se věnuje popisu návrhu nové symetrické blokové šifry, jejími součástmi a vlastnostmi a provedením analýzy rychlosti a výkonnosti navržené šifry s vyvozením závěrů. V další části se zabývá analýzou navržené blokové šifry z pohledu bezpečnosti a rozborem výsledků provedené analýzy. V poslední části se věnuje popisu implementace grafického uživatelského rozhraní pro šifrování a dešifrování souborů a diskuzi nad možnostmi použití navržené blokové šifry pro mobilní zařízení. V práci je navržena originální kryptografická aplikace pro šifrování a dešifrování souborů symetrickou blokovou šifrou. Aplikaci jsem prakticky vyzkoušel a musím konstatovat, že je funkční.

Po formální stránce je práce na vysoké úrovni, neobsahuje téměř žádné pravopisné chyby a překlepy. Práce je zpracována přehledně s logicky navazujícími kapitolami a s velmi dobrou grafickou úpravou. V závěru práce autor srozumitelně a podrobně shrnuje zjištěné poznatky. V diplomové práci autor uvádí adekvátní množství obrázků k objasnění popisované problematiky. Seznam literatury zahrnuje odpovídající množství relevantních zdrojů. Všechny body zadání práce byly splněny.

Diplomant prokázal hluboké znalosti daného tématu a pokročilé programátorské znalosti a dovednosti.

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Při obhajobě prosím o zodpovězení následujících otázek:

1. Vámi navržená kryptografická aplikace neobsahuje validaci (ověření shodnosti) hesla. Můžete vysvětlit proč a případně se vyjádřit, kdy je taková funkcionalita potřebná či nikoliv?

2. Jsou možná nějaká další rozšíření návrhu aplikace?

**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 4.6.2014 Podpis oponenta diplomové práce