

## OPONENTSKÝ POSUDEK BAKALÁŘSKÉ PRÁCE

Student: ŠŮSTAL ONDŘEJ

Oponent: Ing. David Malaník, Ph.D.

Studijní program: Inženýrská informatika  
Studijní obor: Informační a řídicí technologie  
Akademický rok: 2014/2015

Téma bakalářské práce: Aplikace pro kryptoanalýzu substitučních šifer

### Hodnocení práce:

1. Obtížnost zadaného úkolu
2. Splnění všech bodů zadání
3. Práce s literaturou a její citace
4. Úroveň jazykového zpracování
5. Formální zpracování – celkový dojem
6. Logické členění práce
7. Vhodnost zvolené metody řešení
8. Kvalita zpracování praktické části
9. Výsledky a jejich prezentace
10. Závěry práce a jejich formulace
11. Přínos práce a její využití

| A  | B                                   | C                                   | D                                   | E                                   | F                        |
|--|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|
| Hodnocení:<br>A – nejlepší; F - nevyhovující |                                     |                                     |                                     |                                     |                          |
| <input type="checkbox"/>                     | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> |
| <input type="checkbox"/>                     | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/>                     | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> |
| <input type="checkbox"/>                     | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> |
| <input type="checkbox"/>                     | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> |
| <input type="checkbox"/>                     | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> |
| <input type="checkbox"/>                     | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/>                     | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> |
| <input type="checkbox"/>                     | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/>                     | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/> |

### Celkové hodnocení práce:

Výsledná známka není průměrem výše uvedených hodnocení. Znamku 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 bakalářskou práci doporučuji k obhajobě a navrhuji hodnocení**

**D - uspokojivě.**

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

### Otázky k obhajobě:

Tabulka 13 a 14, co znamenají čísla uvedená za bigramy a trigramy? Máte v aplikaci dešifrování PlayFair, ale program šifru nevylušití.

### Další připomínky, vyjádření, náměty k obhajobě práce (možno pokračovat i na další stránce):

Teoretická část odpovídající bodu zadání č. 1 je zaměřena na tvorbu a funkci šifer. Dle zadání by ale měla obsahovat rešerši ke kryptoanalytickým metodám. Návrh aplikace je velmi povrchní. Jedná se o popis aplikace, není tu žádný vývojový diagram, ER diagram, návrh aplikační logiky, atd.. Po formální stránce obsahuje práce hodně překlepů. Bod č. 5 je řešen pouze 8 řádky textu, které ale nepopisují rozšíření aplikace ale možnosti pluginů jazyka Java. Rozsah bodu č. 5 považuji za nedostatečný.

Datum 26.5.2015

Podpis oponenta bakalářské práce