UNIVERZITA HRADEC KRÁLOVÉ
Přírodovědecká fakulta Katedra informatiky

Posudek oponenta bakalářské práce

Název: **Luštění transpozičních šifer s podporou počítače**
Autor: **Sabina Hájková**
Vedoucí ZP: PhDr. Michal Musílek, Ph.D.
Oponent ZP: Ing. Petr Voborník, Ph.D.

Cílem bakalářské práce bylo posoudit možnosti využití počítače jako pomůcky k luštění klasických transpozičních šifer různých typů, s podrobnějším zaměřím na konkrétní typ šifer a metodu jejich analýzy, například na luštění jednoduché sloupcové transpozice nebo Fleissnerovy mřížky na základě slovníkového útoku využívajícího pouze krátkých slov.

Práce je rozčleněna na dva hlavní oddíly a to část teoretickou a část praktickou. Součástí práce je také přiložená vlastní aplikace, rozdělená do třech samostatných souborů/sešitů Microsoft Excel.

V teoretické části (kap. 1) autorka dle různých citovaných zdrojů vysvětluje základní pojmy z oblasti kryptografie a kryptoanalýzy, dějiny tohoto oboru a podrobněji rozebírá tři rozepsané šifry a způsoby jejich luštění. Vysvětlení jsou převážně podána vlastními slovy, stručně, ale srozumitelně a názorně.

Praktická část (kap. 2) popisuje aplikaci vytvořenou ve VBA jako makra MS Excelu. Ta zahrnuje programy pro luštění transpozičních šifer, frekvenční analýzu a jednoduchou sloupcovou transpozici.

Teoretický přehled i popis vlastní aplikace šifrovacích algoritmů jsou napsány velmi zasvěceně. Mezi nedostatky bych uvedl, že některé tabulky a schématické obrázky nemají identifikační číslo a popis, a také že úvodní kapitola je spíše anotací (popisem struktury práce) než úvodem do problematiky. Ocenit je ovšem třeba vytvoření vlastních funkčních a uživatelsky přehledných aplikací, které byly zpracovány v ne zrovna programátorsky nejpřívětivějším prostředí maker Microsoft Excel.

Výsledná práce splňuje stanovené cíle a je bez zásadnějších formálních nedostatků. Doporučuji práci k obhajobě a navrhuji známku **výborně**.

V rámci obhajoby před komisí bych se autorky zeptal, *jaké výhody a nevýhody má tzv. Vernamova šifra*.

V Hradci Králové 15. 5. 2015 Ing. Petr Voborník, Ph.D.