U N I V E R Z I T A H R A D E C K R Á L O V É
Přírodovědecká fakulta Katedra informatiky

Posudek vedoucího bakalářské práce

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

Práce se zabývá vybranými transpozičními šiframi, především jednoduchou sloupcovou transpozicí s úplnou tabulkou a Fleissnerovou otočnou mřížkou, jejich principem, vlastnostmi, postupy šifrování a dešifrování a metodami jejich luštění. Významnou součástí práce je aplikace, kterou autorka samostatně navrhla, naprogramovala a odladila, která prostřednictvím počítače provádí popsané algoritmy, a tak výrazně usnadňuje a urychluje činnost člověka.

Vlastní práce má 36 stran textu, doplněného pěti stranami příloh s vývojovými diagramy klíčových algoritmů. Text je stručný, jasný a výstižný, podává ucelený přehled typů klasických šifrových systémů, vhodným způsobem implementuje tradiční algoritmy do podoby maker pro tabulkový procesor MS Excel. Právě u transpozičních šifer je použití tabulkového procesoru velmi vhodné, protože tabulky se tradičně využívaly i pro šifrování, dešifrování a luštění nástroji tužka a papír. Počítač zde působí jako „katalyzátor“, který tradiční postupy usnědňuje a výrazně urychluje.

V úvodu autorka vhodně formuluje cíle práce a stanovuje snadno kontrolovatelná kritéria jejich splnění. Hlavním cílem teoretické části práce je podat přehled základních částí klasické kryptologie a stručně zmapovat vývoje ručích šifer na základě výběru konkrétních, historicky významných systémů a popisu metod jejich luštění. Cílem praktické práce je vytvoření počítačové aplikace která by sloužila k šifrování a dešifrování metodami jednoduché sloupcové transpozice s úplnou tabulkou a Flaissnerovy otočné mřížky a luštění odpovídajících šifrových textů, doplněné o nástroj frekvenční analýzy textu jako základní metody pro ověření skutečnosti, že daný text je zašifrován transpoziční šifrou.

Práce má vhodnou logickou strukturu a dobrou grafickou úroveň. První kapitola představuje teoretickou část práce, definuje základní pojmy, popisuje vybrané substituční a transpoziční šifry a jejich použití k šifrování textu. Druhýá kapitola představuje praktickou část práce a soustředí se na luštění transpozičních šifer s podporou počítače.

Rozsah práce:	36 stran textu, 5 stran příloh a makra v Excelu v programovacím jazyce Vusual Basic for Application
Formální úprava:	odpovídá vnitřním předpisům UHK
Logická struktura:	práce je vhodně členěna do kapitol a podkapitol
Bibliografické citace:	odpovídají normě ČSN ISO 690, 8 knižních a 18 on-line zdrojů
Cíle práce:	cíl práce je jasně deklarován v úvodu práce, v závěru práce autorka konstatuje jeho splnění

Z hlediska vlastního přínosu autora je stěžejní praktická část práce, tedy jednak druhá kapitola bakalářské práce a jednak vlastní tabulková aplikace. Na základě předložené práce konstatuji, že autorka splnila vytčené cíle. Práci doporučuji připustit k obhajobě a navrhuji hodnocení výborně.

V Hradci Králové dne 17. 5. 2015