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 kybernetiky

Posudek vedoucího bakalářské práce

Název: **Počítačová analýza šifrované korespondence rodu Piccolomini**
Autor: **Václav Vlnas**
Vedoucí : **PhDr. Michal Musílek, Ph.D.**
Oponent: **doc. RNDr. Štěpán Hubálovský, Ph.D.**

Bakalářská práce zajímavým a netradičním způsobem propojuje oba obory studované autorem práce – informatiku a historii. Archivy, zejména archivy šlechtických rodů, jejichž příslušníci zastávali důležité státní, vojenské či diplomatické pozice, obsahují kromě listin psaných otevřeným textem také šifrované listiny. Analýza takových textů je komplexním úkolem, který je tradičně nutné provádět z velké části ručně, např. rozpoznávat různé podoby psaného písma (různých druhů kurentu, či speciálních šifrových znaků), počítat frekvence jednotlivých znaků apod., ve kterém může některé monotónní úkoly provádět počítač. Autor práce vhodně využil vlastnoručně vytvořených maker v jazyce Visual Basic for Applications, aby šifrové texty, přepsané do tabulek Excelu, dešifroval. Po určení daného šifrového systému a určení převodové tabulky se totiž jedná o ryze mechanickou záležitost. Makra jsou psána takovým způsobem, aby umožnila postupné odkrytí převodových tabulek a tím účinné podporovala luštitele šifer ve fázi postupné rekonstrukce šifrovací tabulky.

V úvodu práce autor objasňuje motivaci k volbě tématu a formuluje cíl práce a popisuje rozvržení textu do jednotlivých kapitol. První kapitola představuje stručný úvod do klasické kryptologie a seznámení s vybranými typy ručních šifer. Druhá kapitola stručně seznamuje s tabulkovým procesorem Excel a programovacím jazykem Visual Basic for Applications, který následně používá k tvorbě dešifrovacích maker a maker pro frekvenční analýzu šifrových textů. Třetí kapitola je historickým exkurzem, popisujícím vzestup rodu Piccolomini od 13. století, přes členy rodiny, kteří usedli na papežském stolci až k Otaviovi Piccolomini, polnímu maršálu císařských vojsk, který se po třicetileté válce usadil na panství v Náchodě, které získal za své věrné služby říši. Tak se šifrované dopisy adresované Otaviovi Piccolomini dostaly do Čech, kde jsou v současné době uloženy ve Státním oblastním archivu Zámrsk. Práce v badatelně archivu a postup hledání šifrových dokumentů s využitím tzv. archivních pomůcek je popsána v závěru třetí kapitoly.

Praktickou částí a původním prakticky použitelným výstupem práce je čtvrtá kapitola práce, kde autor analyzuje postupně čtyři různé šifrové texty. V každé z podkapitol seznamuje s použitým typem šifry, rekonstruuje převodovou tabulku příslušné substituce, uvádí a vysvětluje kód makra použitého pro dešifrování a makra pro frekvenční analýzu textu, na závěr uvádí výsledek frekvenční analýzy a určuje použitý jazyk. Čtením dešifrovaného, tedy otevřeného textu a také souladem s výsledky frekvenční analýzy (kdy rozložení frekvencí jednotlivých písmen abecedy je typické pro určitý jazyk) došel autor k závěru, že první šifra vznikla šifrováním francouzského textu a další tři pak šifrováním textu italského. První tři texty se podařilo dešifrovat na 100 %, poslední pak z 95 %. Smysl textů lze při jejich čtení zhruba určit, přesný překlad ani zasazení textů do konkrétních událostí třicetileté války nebylo cílem této práce.

V závěru autor shrnuje výsledky práce, konstatuje splnění vytyčeného cíle, hodnotí pozitivní přínos badatelské i programátorské činnosti pro osobní rozvoj a vyjadřuje potřebu v započaté práci v budoucnu pokračovat

.

Rozsah práce:	58 stran textu, 14 stran příloh, rozsáhlá elektronická příloha
Formální úprava:	odpovídá vnitřním předpisům UHK
Logická struktura:	práce je vhodně členěna do kapitol a podkapitol
Bibliografické citace:	odpovídají normě ČSN ISO 690, 12 knih, 4 on-line články
Cíle práce:	cíl práce je jasně deklarován v úvodu práce, v závěru práce autor konstatuje jeho splnění

Teoretická část práce podává ucelené a přesné východisko k počítačem podporované analýze šifrových textů daného typu. Z hlediska vlastního přínosu autora je významná praktická část práce. Na základě předložené práce konstatuji, že autor splnil vytčené cíle. Práci doporučuji připustit k obhajobě a navrhuji hodnocení A.

V Hradci Králové dne 21. 5. 2017