

Posudek oponenta bakalářské práce

Název: Historie šifrování

Autor: Pavel Musílek

Vedoucí ZP: doc. RNDr. Štěpán Hubálovský, Ph.D.

Oponent ZP: Mgr. et Bc. Radek Němec, Ph.D.

Cílem bakalářské práce bylo podat ucelený přehled vývoje a základních typů klasických ručních šifer. V praktické části bylo cílem vytvořit studijní materiál podporující využití klasických ručních šifer ve výuce informatiky formou sady pracovních listů s úlohami různé obtížnosti.

Autor má rozdělenou práci do několika kapitol, kde v teoretické části seznamuje čtenáře se základními kryptologickými pojmy a historií šifrování. V praktické části jsou pak vytvořeny praktické listy, kterou jsou koncipovány tak, aby měl žák možnost dozvědět se něco z dobového kontextu dané šifry, pochopit její princip a prakticky aplikovat, co se naučil.

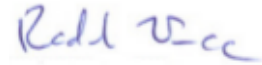
Výsledkem je práce popisující základy kryptologii. V teoretické části oceňuji podrobně popsané základní pojmy kryptologie a historii šifer a jejich luštění od počátku výskytu šifrování až po novodobé dějiny. Kladně hodnotím spojení šifer s historickým kontextem dané doby. V praktické části práce oceňuji praktické listy, kterou jsou tvořeny formou modelových příkladů bitev. Čímž má žák možnost se na krátký okamžik přenést do dávno minulé doby, vžít se do role vojevůdce a kryptografa, který rozhoduje o výsledku bitvy, což jej podněcuje k vyššímu úsilí o zdoání problému. Jako záporné považuji nesprávnou terminologii termínů příklad a úloha. Zejména v pracovních listech by měl být použit správný termín.

Celkově práci hodnotím jako velmi zdařilou a doporučuji v ní pokračovat v rámci diplomové práce, kde se bude autor zaměřovat na ověření praktických listů ve výuce.

Konkrétní připomínky k diskusi:

1. Zkoušel jste pracovní listy někomu poskytnout pro ověření jejich funkčnosti, s jakým výsledkem jste se setkal?

Přes uvedené připomínky práce splňuje požadavky kladené na bakalářskou práci, a proto doporučuji práci k obhajobě a navrhuji známku **B**.



V Hradci Králové 22. 5. 2017

Mgr. et Bc. Radek Němec, Ph.D.