Posudek vedoucího na diplomovou práci

Jiřina Hrušová, Kryptografie na střední škole

Práce se skládá ze dvou hlavních částí. První část je text o klasických a moderních šifrovacích metodách určený středoškolákům, druhá část se pak věnuje aplikacím teorie informace na testy s uzavřenými otázkami.

První část je napsána čtivě a do velké míry splňuje svůj účel. Pár námitek mohu mít k některým formulacím, které do určité míry odrážejí nedostatečně ujasněnou terminologii. Uvedu je v závěru posudku. Zde pouze k výběru témat. Kapitola o kvantové kryptografii mi přijde myšlenkově o dost náročnější než ostatní témata. Osobně bych ji do textu určeného pro středoškoláky zařadil v mnohem omezenější míře.

Ve druhé části autorka napřed jasně a srozumitelně ukazuje informační chudobu odpovědí na multiple-choice test. Ukazuje možné způsoby kódování těchto odpovědí. Za výborný považuji nápad s využitím hexadecimální soustavy. V páté kapitole pak shrnuje informace ze svého webového formuláře, prostřednictvím kterého sbírala informace o možnostech komunikace správných odpovědí v multiple-choice testech. Dále uvádí popis jednoho experimentu, který uskutečnila na škole, na které učí. Výsledky experimentu a sbírání odpovědí jsou do velké míry ovlivněné krátkostí času, který si autorka na tuto část diplomové práce ponechala. Jakkoliv je výsledek experimentu ve spolupracující třídě výmluvný, chtělo by to ještě jej doplnit více podobnými experimenty, obměňovat jejich podmínky, např. použít klasické školní rozdělení na varianty A a B, aby se znesnadnily možnosti komunikace mezi žáky, použít dozor, který by byl zcela neinformovaný, pokud jde o možnosti skryté komunikace mezi žáky, apod. Přes tyto nedostatky experimentální části si myslím, že výsledky by měly být zveřejněny, např. na portálu Česká škola.

A nyní některé připomínky.

Některé problémy v první části podle mého názoru vyplývají z ne zcela jasné formulace faktu, že šifrový text vytvořený danou šifrou závisí na dvou parametrech – na otevřeném textu a na klíči. Tak například při popisu knižní šifry je na str. 11 uvedeno: *„Tato jednoduchá metoda šifrování je speciální případ Vigenerovy šifry s předem dohodnutým klíčem."* Hned v následující větě sice autorka uvádí předchozí větu na pravou míru tím, že zdrojem klíču je předem domluvená kniha z domácí knihovny, ale citovaná formulace je přinejmenším zavádějící. Knižní šifra nemá předem dohodnutý klíč, ale zdroj klíčů.

Na str. 13-14 při popisu Vernamovy šifry bych jako hlavní problém spíš viděl skutečnost, že je třeba předat bezpečným kanálem druhé straně klíč, který má stejnou délku jako šifrovaná zpráva. Proto je možné Vernamovu šifru používat pouze v situacích, kdy je bezpečný kanál k dispozici, např. v podobě diplomatického zavazadla. Problém s náhodností klíče vzniká pouze tehdy, když bezpečný kanál k dispozici není a předává se pouze jakýsi zárodek klíče, ze kterého je potom klíč generován předem dohodnutým generátorem pseudonáhodných znaků. Bezpečnost Vernamovy šifry pak závisí na kvalitě tohoto generátoru.

Na str. 14 bych asi neformuloval větu *„Jak lze převést Vernamovu šifru na knižní?"* Vernamova šifra obecně nemá s knižní šifrou nic společného. Pouze v případě, kdy jsou dva texty zašifrované stejným klíčem, lze odečtením těchto dvou šifrových textů dostat jeden

šifrový text, kdy jeden z původních otevřených textů je použit jako klíč k zašifrování druhého otevřeného textu knižní šifrou.

Pravý sloupec horní tabulky na str. 16 je nadbytečný v tom, co má tabulka sdělit – jak vypadá operace XOR.

Část o Enigmě by měla předcházet část o binárním kódování, bylo tomu tak historicky a je tomu tak i obsahově. Binární kódování přišlo až s počítači. K části o Enigmě lze mít mnoho připomínek, je psána opravdu „lehkým" stylem nebo „horkou jehlou". Stačí si jenom přečíst první dva odstavce a pak poslední dva odstavce. Vyjasnit si, co chce autorka vlastně vyjádřit, není vůbec jednoduché. Hlavní faktickou námitku lze mít v tom, že konstruktér Enigmy se jmenoval Arthur Scherbius a ne Schrebius (i když chybné jméno s překlepem diplomantka asi převzala z mých textů na webu).

Autor šifry Lucifer se jmenoval Horst Feistel, nikoliv Feistler.

Nevím, jak mám rozumět větě na str. 20 těsně před formulí (5) *„ ...ale nakonec se podařilo takovou funkci, která splňuje požadavky symetrické šifry:"* Asi mělo být „...ale nakonec se podařilo **najít** takovou funkci, která splňuje požadavky **pro jednosměrnou funkci**:".

Také ve třetí kapitole má občas autorka problémy s jasným vyjadřováním. Tak např. první věta třetího odstavce na str. 29: *„Přiřazením posloupnosti znaků z množiny Z prvkům množiny M vznikne kódové slovo w_i, ...".* Prvkům množiny M ani nepřiřazujeme jednu posloupnost ani jenom jedno kódové slovo!

Neformální vyjádření typu „nejmenší počet bitů, do kterých uložíme prvky množiny" (str. 30 pod první tabulkou) lze také formulovat tak, aby byla současně srozumitelná i matematicky obhajitelná.

Předložená práce splňuje požadavky na diplomovou práci, proto navrhuji, aby byla jako diplomová práce uznána a navrhuji hodnotit ji známkou **výborně.**

V Praze, 15.5.2006

Doc. RNDr. Jiří Tůma, DrSc.