Posudek na diplomovou práci

Jiřina Hrušová: Kryptografie na střední škole

Předložená práce sestává celkem ze sedmi kapitol. Název je mírně zavádějící, hlavním tématem jsou totiž tzv. multiple-choice testy, tj. testy určené k prověřování znalostí, ve kterých studenti vybírají z několika nabídnutých odpovědí.

První kapitola vysvětluje pojmy kódování zpráv (jde o reprezentaci zprávy pomocí dohodnuté množiny symbolů, např. v Morseově abecedě nebo ve dvojkové soustavě pomocí ASCII tabulky) a šifrování zpráv (utajení obsahu zprávy před nepovolanými osobami).

Nejrozsáhlejší druhá kapitola je věnována historii šifrování, od jednoduché Caesarovy šifry až po prakticky neprolomitelnou Vernamovu šifru. 20. století znamenalo nástup strojového šifrování; připomenuta je např. známá Enigma, ale především moderní počítačové kryptografické algoritmy (např. DES, RSA). V závěru kapitoly je zmíněna kvantová kryptografie jako možná budoucí alternativa.

Třetí kapitola rozebírá kódování informací, především ve dvojkové soustavě. Zde se také poprvé setkáváme s multiple-choice testy. Autorka ukazuje způsob, jak si studenti mohou poměrně efektivně předávat výsledky – jednou číslicí v šestnáctkové soustavě lze totiž kódovat odpovědi na 2 otázky (jsou-li nabízeny vždy 4 možné odpovědi).

Čtvrtá kapitola shrnuje některé poznatky z teorie informace, např. Shannonovu definici entropie a Huffmanův algoritmus optimálního kódování.

Zbývající tři kapitoly jsou již věnovány multiple-choice testům. Autorka se snažila ukázat, že tento druh testů nemá příliš velkou vypovídací hodnotu, neboť umožňuje studentům snadné předávání výsledků. Hypotézu se pokusila ověřit na studentech střední školy, které vyškolila v metodách napovídání, a poté sledovala, zda dojde ke zlepšení výsledků při použití multiple-choice testů.

Experimenty byly velmi pečlivě připraveny a jejich výsledky přehledně znázorněny. Ukázalo se, že pokud jsou studenti dostatečně motivováni a vyškoleni v metodách napovídání, pak se jejich výsledky skutečně zlepší.

Diplomová práce je velmi pěkně vysázena, tento dojem však poněkud kazí větší množství pravopisných chyb. Kapitola o historii šifer je napsána velmi poutavě, autorka ale neuvedla, odkud čerpala informace. Jde o *Knihu kódů a šifer* zmíněnou v seznamu literatury?

Dále mám pocit, že obsah kapitol 2 a 4 příliš nesouvisí s vlastním tématem diplomové práce – pochybuji, že by studenti při sdělování výsledků používali Huffmanovo kódování nebo některou z šifer uvedených v kapitole 2. Více místa mohlo být věnováno samotným multiple-choice testům; postrádal jsem např. podrobnější informace o tom, jak probíhalo školení studentů v metodách napovídání.

I přes tyto nedostatky považuji předloženou práci za nadprůměrnou. Doporučuji uznat ji za diplomovou práci a navrhuji hodnocení *výborně*.

V Praze dne 9. 5. 2006

RNDr. Antonín Slavík, Ph.D.