KATEDRA INFORMATIKY
UNIVERZITA PALACKÉHO V OLOMOUCI
www.inf.upol.cz

Posudek bakalářské práce

Název práce:	Asymetrické šifrování
Autor práce:	Pavel Urbášek
Vedoucí práce:	RNDr. Eduard Bartl, Ph.D.

Splnila práce cíle uvedené v zadání?
ano

Jazyková úroveň práce:
dobrá

Formální zpracování:
podprůměrné

Komentáře a připomínky:

Program je velmi jednoduchý. Jeho využití jako demonstračního nástroje, pomocí kterého by uživatel pochopil vybrané asymetrické šifry a jejich prolamování, je diskutabilní. Jako nevyhovující vidím funkcionalitu prolomení šifry RSA (pro malé moduly). Uživatel totiž nemá možnost ověřit, jestli byl modul skutečně rozložen na součin dvou prvočísel, nebo jestli byla tato čísla získána ze vstupu.

Text práce je po jazykové stránce pěkný, obsahuje však mnoho typografických chyb. Matematické partie jsou psány neobratně, navíc se občas vyskytují i faktické chyby. Jako příklad uvádím definici multiplikativní inverze v $\mathbb{Z}_n$ na str. 20 (zde se však může jednat o překlep). Dalším příkladem je tvrzení na str. 45 říkající, že faktorizace přirozeného čísla na součin prvočísel je NP-úplný problém. Zmíněná faktorizace totiž není rozhodovacím problémem, takže nemá smysl mluvit o NP-úplnosti; navíc ani o rozhodovací verzi tohoto problému v současnosti s jistotou nevíme, jestli je NP-úplná.

Kladně hodnotím, že byly do textu zařazeny některé zajímavé partie týkající se asymetrických šifer.

Celkové hodnocení:
E

Je práce vhodná pro propagační účely katedry?[1]
ne

V Olomouci dne 29. srpna 2014
RNDr. Eduard Bartl, Ph.D.
vedoucí práce

[1] odpověď neovlivňuje celkové hodnocení práce