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

Posudek bakalářské práce

Název práce:	Využití prvočísel při šifrování dat
Autor práce:	Matěj Ošťádal
Vedoucí práce:	doc. RNDr. Miroslav Kolařík, Ph.D.

Splnila práce cíle uvedené v zadání?
Ano.

Jazyková úroveň práce:
Dobrá. Občas se objevují menší jazykové chyby nebo překlepy; například hned na začátku textu v definici na straně 9 patří „symetrická šifra“ místo „asymetrická šifra“.

Formální zpracování:
Dobré. Text je hodně fragmentovaný, velmi často se objevují odstavce obsahující jedinou větu. Občas se vyskytují drobné typografické chyby.

Komentáře a připomínky:
Tematicky se mi zdá být práce poněkud neukotvená. Její název je sice „Využití prvočísel při šifrování dat“, ale většina textu je věnována samotnému šifrování, což je patrné již z názvů kapitol (1. Symetrické šifrování; 2. Asymetrické šifrování; 3. Kryptografie a kvantové počítače; 4. Eliptické křivky).

Definice šifer by se dala zjednodušit tak, že by se místo abecedy znaků uvažovala množina číselných kódů těchto znaků. Pak by bylo možné například u Caesarovy šifry pracovat přímo s množinami zbytkových tříd $\mathbb{Z}_n$, kde n je počet znaků abecedy. Namísto komplikovaného zápisu nosných množin $(\mathbb{N}_0, \Sigma, \Sigma)$[1] by pak bylo možné psát $(\mathbb{Z}_n, \mathbb{Z}_n, \mathbb{Z}_n)$.

Domnívám se, že definice dokonalého šifrování na straně 13 je chybná. Uvedená definice je dokonce v rozporu s korektností šifry.

Rád bych se studenta zeptal, jestli při implementaci šifry RSA používal nějaké algoritmy urychlující umocnění v modulární aritmetice, které má nepříznivou časovou složitost. Pohledem do zdrojového kódu jsem nabyl dojmu, že je využito pouze pythonovské funkce `pow`.

Celkové hodnocení:
Velmi kladně hodnotím, jak si student poradil s tématem, které obtížností spadá spíše do magisterského studia. Sympaticky také působí velký rozsah textu, ze kterého je patrný velký časový vklad vnesený do jeho tvorby. Práci považuji navzdory svým kritickým poznámkám za zdařilou, navrhuji známku B.

V Olomouci dne 27. května 2023
RNDr. Eduard Bartl, Ph.D.
oponent

[1] V textu práce se navíc píše $(\mathbb{N}_0, \Sigma^L, \Sigma^L)$, což není typově správně, jak je vidět ze vztahů na straně 10.