



HODNOCENÍ ZÁVĚREČNÉ KVALIFIKAČNÍ PRÁCE POSUDEK VEDOUCÍHO

Autor závěrečné práce: Bc. David Salač

Vedoucí práce: doc. RNDr. Miroslav Koucký, CSc.

Název práce: Distributed application for cryptanalysis of public-key cryptosystems

A. Úplnost abstraktu, klíčová slova odpovídají náplni práce	Výborně minus (1-)
B. Kvalita zpracování rešerše	Výborně minus (1-)
C. Řešení práce po teoretické stránce	Výborně minus (1-)
D. Vhodnost, přiměřenost použité metodiky	Výborně minus (1-)
E. Úroveň zpracování výsledků a diskuse	Velmi dobře (2)
F. Vlastní přínos k řešené problematice	Velmi dobře (2)
G. Formulace závěru práce	Velmi dobře (2)
H. Splnění zadání (cílů) práce	Splněno
I. Skladba, správnost a úplnost citací literárních údajů	Výborně minus (1-)
J. Typografická a jazyková úroveň (vč. pravopisu)	Velmi dobře minus (2-)
K. Formální náležitosti práce (struktura textu, řazení kapitol, přehlednost ilustrací)	Výborně minus (1-)
L. Přístup studenta k řešení (samostatnost, aktivita...)	Výborně (1)

Komentáře či připomínky:

Student si jako jazyk práce zvolil angličtinu, což vzhledem k tématu DP lze považovat za velmi rozumné. Nicméně je třeba konstatovat, že práce obsahuje řadu gramatických chyb, které však nejsou zásadní překážkou pro srozumitelnost textu.

Práce obsahuje několik věcných chyb. Jak vyplynulo z konzultací, lze naprostou většinu z nich považovat za překlepy.

...pokračuje na straně 2





Celkové zhodnocení:

Téma DP je iniciativou studenta, což se velmi pozitivně projevilo na spolupráci. Student pracoval značně samostatně, intenzivně a prokázal předpoklady pro vědeckou práci.

Téma DP je aktuální a z teoretického i aplikačního hlediska náročné. Student prostudoval relevantní a poměrně rozsáhlou anglicky psanou odbornou literaturu (větší rozsah, než odpovídá rozsahu DP) a porozuměl náročnějším partiím teorie čísel a aplikované kryptologie.

Lze konstatovat, že cíle DP byly splněny.

Otázky k obhajobě:

1. Výpočet logaritmu reálného čísla je v podstatě jednoduchá záležitost. Stručně a jednoduše objasněte, v čem spočívá problém výpočtu diskrétního logaritmu právě ve srovnání s výpočtem logaritmu reálného čísla.
2. Ověřoval jste správnost výpočtů? Pokud ano, jak. Např. u metody RSA uvádíte příklady, které pro dešifrování vyžadují výpočet modulární mocniny, jejíž základ, exponent i modul jsou relativně velká přirozená čísla (sedmdesáti i vícemístná apod.).

Celková klasifikace:

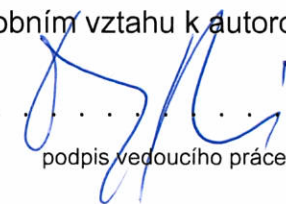
Práce splňuje požadavky na udělení akademického titulu, a proto ji doporučuji k obhajobě

Navrhuji tuto práci klasifikovat stupněm Výborně minus (1-)

V Liberci

dne 31. 5. 2017

Podpisem současně potvrzuji, že nejsem v žádném osobním vztahu k autorovi práce


.....
podpis vedoucího práce