POSUDEK OPONENTA NA BAKALÁŘSKOU PRÁCI ADAMA CHRISTOVA *STATISTICKÉ TESTY HAŠOVACÍCH (=ŽVÝKACÍCH) FUNKCÍ*

Předkládaná práce obsahuje (kromě žertovného pokusu o překlad slova hash v názvu) základní popis hašovacích funkcí, podrobný popis hašovací funkce MD5 a statistické testy zaměřené na některé její vlastnosti částečně s ohledem na nedávné úspěšné útoky na tuto funkci.

Práce je napsána velmi přehledně, oceňuji srozumitelný popis poměrně komplikované struktury funkce MD5.

Rovněž prováděné testy jsou zajímavé a jsou popsány korektně. V tomto případě by se chtělo říci, že až příliš korektně. Popis testů je totiž psán v čistě odborné terminologii matematické statistiky bez bližšího rozboru, vzniká dojem, že text je dosti doslovně převzat z literatury, na kterou je odkazováno. Zbývá doufat, že uchazeč rozumí tomu, co se za vzorečky skrývá, tedy tomu, co vlastně testuje. Podrobnější vysvětlení vlastními slovy by bakalářské práci slušelo.

Statistika je ovšem v práci přece jen pouze nástrojem. Ještě citelnější je proto nedostatečné vysvětlení toho, proč jsou testované vlastnosti pro hašovací funkci důležité. Proč by funkce nebyla bezpečná, pokud by výstupní bity nebyly náhodné (podobně pro ostatní testy)? Tento nedostatek se projevuje i v dosti bezelstném hodnocení výsledků, které je v kontrastu se sofistikovaným statistickým aparátem: „Analyzováním výsledků zjistíme, že na obou hladinách jsou četnosti zamítnutí poměrně malé, tudíž tyto případy nemají žádný statistický význam“ (str.14, podobně na str. 16). Kolik zamítnutí by už mělo statistický význam? A především, jaké by to mělo důsledky pro kryptografické vlastnosti funkce?

Naopak oceňuji, že si uchazeč všiml asymetrie výsledků u Stevensových a Klímových podmínek (str. 26 dole). Sledování podobných postřehů by mohlo vést k zajímavým zjištěním.

Oponent si ještě povšiml jedné gramatické chyby: str. 19, ř. 8, namísto „jí“ má být „ji“.

Práce splňuje požadavky kladené na bakalářskou práci a doporučuji ji k obhajobě.

Navrhuji hodnocení „velmi dobře“.

Praha 6. září 2006

Štěpán Holub