Posudek

❑vedoucího ❑**oponenta**
❑**diplomové** ❑bakalářské práce
Autor/Autorka: Barora Galaczová
Název práce: Bezpečnost a použitelnost základních hashovacích funkcí, zejména MD5, SHA-1 a SHA-2.
Jméno oponenta: Daniel Joščák

Matematická úroveň:
❑vynikající ❑velmi dobrá ❑průměrná ❑**podprůměrná** ❑nevyhovující

Grafická, jazyková a formální úroveň:
❑vynikající ❑**velmi dobrá** ❑průměrná ❑podprůměrná ❑nevyhovující

Výsledky:
❑originální ❑původní i převzaté ❑**netriviální kompilace** ❑citované z literatury ❑opsané

Použité metody:
❑nestandardní ❑**standardní** ❑obojí

Aplikovatelnost:
❑přínos pro teorii ❑přínos pro praxi ❑přínos pro praxi i teorii ❑bez přínosu ❑**nedovedu posoudit**

Věcné chyby:
❑**téměř žádné** ❑vzhledem k rozsahu a pojednávanému tématu přiměřený počet ❑méně podstatné četné ❑závažné

Tiskové chyby:
❑téměř žádné ❑**vzhledem k rozsahu a pojednávanému tématu přiměřený počet** ❑četné

Celková úroveň práce:
❑vynikající ❑velmi dobrá ❑**průměrná** ❑podprůměrná ❑nevyhovující

Práci
❑**doporučuji** ❑nedoporučuji
uznat jako diplomovou. Návrh klasifikace přikládám na zvláštním papíru.

Připomínky a vyjádření vedoucího/oponenta:

Celkovo sa diplomová práca zaoberá popisom a kryptoanalytickým vývojom v najpoužívanejších hashovacích funkciách (h.f.), konkrétne MD5, SHA-1 a funkciách z rodiny SHA-2. Práca má pomerne rozsiahly obsah, preto sa pokúsime k jednotlivým kapitolám vyjadriť postupne.

Po úvodnej kapitole autorka uvádza historický prehľad najpoužívanejších h.f. Vzhľadom na aktuálnosť a počet novovzniknutých h.f. je očakávanie úplného zoznamu nereálne, dovoľujeme si ale upozorniť na absenciu pomerne významnej funkcie RIPEMD-160 (ISO/IEC 10118-3:2003). Táto funkcia vznikla na otvorenej akademickej pôde ako alternatíva k funkciám SHA-1 a 2, vytvorených agentúrou NSA. RIPEMD-160 je schválená pre používanie na všetky kryptografické účely a nachádza sa v implementáciách rozšírených kryptografických knižníc ako sú OpenSSL, Cryptopp, či Java crypto toolkit od IAIK.

V nasledujúcej kapitole je uvedený zoznam neformálnych definícií h.f. a ich vlastnosti. Autorka uvádza základné vlastnosti a konštatuje, že v odbornej literatúre vládne v tejto terminológií pomerná vágnosť, s čím sa dá súhlasiť. Základné definície autorka stručne rozoberá. Oponent práce v tejto kapitole postráda definície na praktické požiadavky pre h.f. ako sú napr. požiadavky na pamäť, rýchlosť, implementovateľnosť, rošíriteľnosť na rôzne výpočtové platformy, ktoré sú hlavným dôvodom, prečo súčasné h.f. nie sú založené na dobre preskúmaných jednosmerných funkciách z teórie výpočtovej zložitosti.

Kapitola 4 rozoberá popis, vývoj kryptoanalýzy a praktické možnosti zneužitia slabín funkcie MD5. Kapitola je založená z veľkej časti na významných publikáciách [11, 37, 17, 7] a je obohatená v kapitole 7 o software na hľadanie kolízií. Výrazne oceňujeme praktickú skúsenosť s implementáciou použitých kryptografických techník, vďaka ktorej je čitateľnosť práce na vysokej úrovni. V časti popisujúcej praktické využitie kolízií autorka ukazuje spôsob vytvorenia kolízie v certifikátoch vložením kolízie do modulu verejného kľúča. Táto metóda je prakticky a technicky výborne popísana, minimálne však krok 4 na str. 32 by si zaslúžil matematicky rigorózny popis a dôkaz správnosti (zostrojenie dvoch RSA modulov n_1 a n_2 s rovnakým suffixom tj. pre 2048 bitový modulov tvaru $n_1 = a_1.2^{1024} + s$, $n_2 = a_2.2^{1024} + s$; $s < 2^{1024}$). K záveru tejto kapitoly si dovoľujeme ešte poznamenať existenciu aplikácií, kde bezkoliznosť MD5 nie je potrebnou vlastnosťou a MD5 sa v nich používa napríklad za účelom generovania psudonáhody alebo urýchlenia vyhľadávania. V týchto prípadoch, je použitie MD5 stále opodstatnené a oceňuje sa jej rýchlosť a rozšírenosť.

Kapitola 5 rozoberá popis, vývoj kryptoanalýzy a budúcnosť funkcie SHA-1. Kryptoanalýza je založená na obdobných technikách ako v prípade funkcie MD5 (resp. SHA-0) a množstvo článkov uvádza, že sú aplikovateľné aj na SHA-1. Reálne toto nebolo ani potvrdené ani vyvrátené, keďže kolízie pre SHA-1 doposiaľ neboli nájdené. Obozretnosť inštitúcií, ktoré nariadili prechod k iným funkciám je správna – napríklad nové podpisy by boli falzifikovateľné. Zároveň je potrebné zôrazniť odolnosť SHA-1 voči nájdeniu druhého vzoru, ktoré by znamenalo neplatnosť súčasných el. podpisov. Autorka toto vhodne a výstižne ukazuje na príklade správ s dĺžkou 2^{64} bitov (≈2 000 000 000 TB). Upozorňuje, že prehnaný pesimizmus, voči dokumentom alebo certifikátom podpísaných pomocou hasha SHA1 dnes, nie je na mieste rovnako.

Kapitola 6 sa zaoberá popisom a postupom vývoja kryptoanalýzy funkcií SHA-2, ktorý v tomto prípade nie je tak rozsiahly a výsledky existujú len pre zjednodušené varianty SHA-2. Jej hodnotnou časťou je podkapitola 6.3, ktorá sumarizuje súčasný stav a odhady použiteľnosti, ktoré sa opierajú o expertný odhad a skúsenosti inštitúcie ETSI s podobnou praxou.

Kapitola 7 dokazuje praktickú schopnosť autorky implementovať kryptoanalytické metódy pre funkciu MD5. Oceňujeme a kladne hodnotíme prehľadnosť a čitateľnsť

zdrojového kódu. Autorka sama uvádza aj dôvod, prečo je jej program pomalší. Je ním overovanie a nastavovanie podmienok v tuneloch. Pre skúseného programátora by táto optimalizácia efektívneho porovnávania a nastavovania na bitovej úrovni však nemala byť problémom a program by dosahoval porovnateľnú rýchlosť s najrýchlejšími tunelovými metódami.

V závere autorka stručne popisuje aktuálny stav súčasných h.f. a stav vývoja vo verejnej súťaži organizovanej úradom NIST o nový štandard SHA-3. Tam je momentálne upretá pozornosť kryptografickej komunity.

Prácu ako celok hodnotím pozitívne. Jej nedostatkami sú absencia vlastných výsledkov, postrádanie presnejšieho zápisu a dôkazu problému (tento stav je v odbore veľmi rozšírený) a zriedkavé preklepy, ktoré ale nijak nebránia čitateľnosti a pochopeniu textu. Autorka v práci ukázala schopnosť naštudovania odbornej literatúry a spracovania pomerne rozsiahleho obsahu článkov. Software, ktorý je súčasťou práce, je ukážkou praktických schopností a ukazuje zvládnutie spomínaných kryptoanalytických techník. Prácu doporučujem uznať ako diplomovú.

V Prešove, 11. 09. 2011

Daniel Joščák