Návrh a kryptoanalýza šifier Zadanie 2

Pavol Sobota
2.10.2022

1 Úvod

Implementácia programu na lúštenie hesiel bola napísaná v jazyku JAVA 17. Knižnica použitá pri hešovaní pomocou SHA256 bola **java.security.** Počítač, ktorí spúšťal implementáciu mal parametre:

- Procesor: Apple M1.
- RAM: 8 GB.
- GPU: Apple M1 7-jadrová GPU.

2 Riešenie

2.1 Redukčná funkcia

Vstup: SHA256 bitový hash v hexadecimálnom formáte Parameter: celé číslo Úlohou redukčnej funkcie bolo predísť vytváraniu hešových cyklov v reťaziach. Ak by sa reťaze so starting point-om A a B stretli v jednom uzli, potom obe reťaze by boli po zvyšok dĺžky rovnaké. Redukčná funkcia bez parametra (parameter 0) zobrala prvých 6 cifier z hexadecimálneho čísla prevedeného do desiatkového a pridala k nim **AIS ID**. Ak mala parameter p tak vybrala každý p-ty prvok z hashu. Napr pre p=2 a SHA256: **2ff1**0**4d**4**d97**306350b162d43f1a239f95a04e785395cebbb7477f1476ddbe417, čislo **2f0dd7** previedla do desiatkovej sústavy a odobrala prvých 6 znakov.

2.2 Hellmanov útok

Pri Hellmanovom útoku sme vytvorili vopred tabuľku hash reťazí vo veľkosti m x t. Prvý prvok reťaze bol náhodne vygenerovaný. Nasledujúce prvky boli vytvorené tak, že predchádzajúci prvok bol zahešovaný pomocou SHA256 a potom bola naň aplikovana Redukčná funkcia bez parametra. Finálny prvok bol v uložený do HashMap¡String, String¿ kde kľúčom bol prvý prvok. Počas útoku sa najprv porovnával hľadaný hash s koncovími prvkami tabuľky. Ak sa zhoda nenašla, zahešoval sa a proces sa opakoval. Ak sa zhoda našla, preiterovaním reťazca v ktorom bola zhoda sa našiel hľadaný otvorený text.

2.3 Rainbow tabuľky

Jediným rozdielom medzi útokom pomocou Rainbow tabuliek a Hellmanovým útokom je v našej práci pridanie parametra do redukčnej funkcie. Veľkosť parametra sa pohybovala od 0 do 63. Odhadovali sme že pomocou tejto zmeny bude menej potenciálnych miest v predgenerovanej tabuľke, kde môžu vzniknúť cykly alebo iné nežiadúce uzly.

	P	T
H m=100 t=100	1,2%	529ms
H m=100 t=10000	0,6%	83min
H m=10000 t=100	6%	16,5s
R m=100 t=100	0,4%	449ms
R m=100 t=10000	0,1%	4min
R m=10000 t=100	0,4%	13,7

Table 1: Tabuľka úspešností a časových zložitostí.

3 Výsledky a Analýza

Skratka H označuje Hellmanov útok, skratka R označuje útok pomocou rainbow tabuliek. P je percentuálna úspešnosť a T čas lúštenia 1000 vzoriek. Z experimentu môžeme usúdiť, že najúspešnejšia TMTO je pri Hellmanovom útoku m=10000 t=100.

4 Záver a Komentár

V práci sme implementovali 2 riešenia problematiky spätného lúštenia hashov pomocou TMTO útokov. Na základe experimentov sme zistili, že efektívnejšie je zvýšiť počet hešových reťazí, ako ich dĺžku. Nedostatky v práci sú nasledovné: Chýba teoretický výpočet. Redukčná funkcia nie je dostatočne náhodná pre zmenšenie potenciálnych prienikov reťazí. Pravdepodobne implementácia rainbow tabuliek je zlá, keďže odsledovaná úspešnosť by sa zrejme dala získať aj náhodným prehľadávaním.

5 Prílohy

Implementácia v jazyku java.
`https://github.com/Nnabuchodonozor/NKS-2022/tree/main/banerow\%20tables`