Návrh a kryptoanalýza šifier

Zadanie 2
Peter Čuřík

Použitý HW a SW na výpočty
HW

SW
Naprogramovanie vlastného riešenia v jazyku Python s pomocou knižnice pycryptodome
Rozdelenie problému medzi virtuálne jadrá CPU

Riešenie 1
Postup
-- hľadanie zhody r(y) medzi všetkými endpointami
-- v prípade neúspechu brute-force prehľadávanie celej tabuľky pomocou rekonštrukcie všetkých chainov od startpointu po endpoint
-- výpočtovo náročné riešenie (trvanie ~16h pre tabuľku b) alebo c))

Redukčné funkcie
Hellman: convertToDecimal(SHA256(i)) % 1 000 000
- kde i je element chainu

Rainbow: convertToDecimal((SHA256(i)) % 1 000 000) + p) % 1 000 000
- kde i je element chainu, p je meniaci sa parameter, rastúci od 0 po t, kde t je dĺžka chainu

Výsledky

Hellmanove tabuľky	Teoretická percentuálna úspešnosť	Percentuálna úspešnosť experimentu	Priemerná doba vyhľadania vzoru	Trvanie experimentu
m = 100, t = 100	0,8%	1,6%	31,5s	8,5m
m = 100, t = 10000	80%	2,2%	46m	17h
m = 10000, t = 100	80%	12,2%	7,6m	15,5h

Rainbow tabuľky	Teoretická percentuálna úspešnosť	Percentuálna úspešnosť experimentu	Priemerná doba vyhľadania vzoru	Trvanie experimentu
m = 100, t = 100	0,8%	0,1%	12,7m	12,7m
m = 100, t = 10000	80%	0,0%	N/A	17,1h
m = 10000, t = 100	80%	1%	1,7h	17,3h

Riešenie 2 (optimalizácia Hellman tabuliek)
Postup
-- hľadanie zhody r(y) medzi všetkými endpointami
-- v prípade neúspechu aplikovanie g funkcií na r(y) najviac t krát - až po nájdenie endpointu
    -- potom presun na startpoint a výpočet prvku pred r(y)
-- "správne riešenie", časovo efektívne
-- všetko ostatné (vrátane redukčnej funkcie) rovnaké ako pri Riešení 1

Výsledky

Hellmanove tabuľky	Teoretická percentuálna úspešnosť	Percentuálna úspešnosť experimentu	Priemerná doba vyhľadania vzoru	Trvanie experimentu
m = 100, t = 100	0,8%	1,2%	0,83s	10s
m = 100, t = 10000	80%	N/A	N/A	N/A
m = 10000, t = 100	80%	3,9%	0,9s	35s

Komentáre:
-- chyba pri implementácii Rainbow tabuliek: odchytený ciphertext bol vždy podrobený prvej zo všetkých redukčných funkcií - to vysvetľuje silno pesimistické výsledky a rozpor s teoretickými očakávaniami
-- chyba pri návrhu parametrizovateľnej redukčnej funkcie pre Rainbow tabuľky, nedostatočne "náhodná"
-- pokus s m = 100, t = 10000 pre Riešenie 2 nestihol včas ukončiť svoj beh