Реалізація атаки Хеллмана на геш-функції

Варіант 9

1 Мета роботи

Набуття навичок реалізації атаки Хеллмана на геш-функцію RIPEMD-320.

2 Хід роботи

Лабораторна робота (спрощений варіант) була виконана не з параметрами, які вказані в методичці, лише перша атака. Оскільки дуже погано реалізована вбудована геш-функція.

Реалізація першої атаки займає багато часу, якщо говорити про другу атаку ДУЖЕ-дуже багато часу (краще не запускати), але я висиділа(.

- Таблиця передобчислень для першої атаки будувалась з параметрами $K = 2^{10}, 2^{12}, 2^{14}$, $L = 2^5, 2^6, 2^7$ Використовується геш-функція усічена до 16 бітів.

- Таблиці передобчислень для другої атаки будувались з параметрами$K = 2^5, 2^6, 2^7$, $L = 2^4, 2^5, 2^6$. Також використовується геш-функція усічена до 16 бітів.

3 Теоретичні відомості

Атака Хеллмана визначається параметрами K — кількістю ланцюгів передобчислень, та L — довжиною ланцюга. Атака складається з двох частин: побудови таблиці передобчислень та її застосування для пошуку прообразу заданого геш-значення.

Для побудови таблиці передобчислень використовується так звана функція надлишковості — відображення $R : V_n \to V_{128}$.

За теоремою Хеллмана середня ймовірність успіху атаки

$$p_{\text{succ}} \geq \frac{1}{N} \sum_{i=1}^{K} \sum_{j=0}^{L-1} \left(1 - \frac{iL}{N}\right)^{j+1},$$

де $N = |f(X)|$ — кількість можливих вихідних значень.

Для t таблиць передобчислень маємо:

$$P_{\text{success}} = 1 - (1 - p_{\text{success}})^t$$

4 Особливості

При виконанні лабораторної роботи використовувалась функція надлишковості, яка генерувала $128 - n$ випадкових бітів і потім до них конкатенувала задане значення:

- r — випадковий вектор довжини $128 - n$ бітів;
- Для довільного вхідного значення $x : R(x) = r \| x$.

Основна особливість лабораторної — використання параметрів таблиці не як сказано в методичці(Це не реально), а спроба в експеримент і комбінування різних параметрів.

А взагалі проблема просто в бібліотечній геш-функції RIPEMD-320. Хтось не зміг її нормально реалізувати.(

5 Приклад виконання атаки

За допомогою таблиці з параметрами $L = 2^{10}, K = 2^5, N = 10000$ була здійснена атака. Перший успіх на спробі 26:

Повідомлення: 13fe05a8c6b2f067257ac53b7b1d0f5c54cc42ef9ff25f66cf22f4926a92d83a

Геш-значення: 49f0a5573128cca5e3b65a90eef9c016c5b7b22ca9423dd9dee2f3849ce463b074a4bac84f6a9ee4

Прообраз:f555f5d9cb837cb744caca4fabc218ee

Перевірка геш-значення: ebdfa10fe9789011b112928ef1f549bf6280c2a706d42db72002f5d7eca043e65bc7d1c9d1b59ee4

6 Результати Першої атаки

L/K	2^{10}	2^{12}	2^{13}
2^5	0.084 %	0.090 %	0.110 %
2^6	0.050 %	0.055 %	0.060 %
2^7	0.030 %	0.031 %	0.029 %

Табл. 1: Теоретичні оцінки успіху атаки

L/K	2^{10}	2^{12}	2^{14}
2^5	0.079 %	0.085 %	0.102 %
2^6	0.047 %	0.052 %	0.058 %
2^7	0.031 %	0.026 %	0.029 %

Табл. 2: Практичні оцінки успіху атаки

Отже, можна побачити, що отримані практичні оцінки майже схожі на теоретичні.

7 Результати Другої атаки

L/K	2^5	2^6	2^7
2^4	74.2 %	98.9 %	99.9 %
2^5	82.1 %	99.0 %	99.9 %
2^6	75.8 %	96.4 %	99.9 %

Табл. 3: Теоретичні оцінки успіху атаки

L/K	2^5	2^6	2^7
2^4	63.1 %	97.6 %	100 %
2^5	75.4 %	99.1 %	100 %
2^6	69.7 %	100 %	100 %

Табл. 4: Практичні оцінки успіху атаки

Отже, тут моєму ноуту стало дуже погано. Можна побачити, що отримані практичні оцінки також майже схожі на теоретичні.

8 Висновки

Після кількох десятків годин експериментів були отримані практичні результати для двох варіантів атак, які можна порівняти з теоретичними і начебто не все погано(тільки ноуту).