Геш-функції та коди автентичності

Домашній комп'ютерний практикум №2

Геш функція згідно варіанту RIPEMD-320

ФІ-03 Кобець Денис

Мета роботи

Опанувати методи оптимізованого перебору для побудови атак на геш-функції, експериментально визначити параметри методу Хеллмана.

Хід роботи

Основне завдання практикуму: реалізувати алгоритм випадкового пошуку прообразів геш-функції на основі таблиць передобчислень та компромісу «час/пам'ять» (атака Хеллмана). Для даного завдання використовується геш-функція h(x), усічена до 32 бітів (тобто n=32).

1. Опис атак, теоретичні оцінки для імовірності успіху (за теоремою Хеллмана)

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 деякого геш-значення.

Для побудови таблиці передобчислень використовується так звана *функція надлишковості* – відображення $R: V_n \to V_{128}$, яке задається вами. Рекомендовано будувати функцію надлишковості таким чином:

– згенерувати випадковий вектор r довжини 128-n бітів, зафіксувати його значення;

– для довільного вхідного значення x покладати $R(x) = r||x$.

Теоретичні оцінки для імовірностей успіху за теоремою Хеллмана:

$$P_{succes} \geq \frac{1}{N}\sum_{i=1}^{m}\sum_{j=0}^{t-1}\left(1-\frac{it}{N}\right)^{j+1}, \qquad N = |f(X)| - \text{кількість можливих виходів}$$

Отримані значення для K- кількістю ланцюгів передобчислень 2^{20}, L – довжиною ланцюга 2^{10}:

$$P_{succes} \geq 3.15236 * 10^{-30}$$

$K = 2^{22},\ L = 2^{11}$:

$$P_{succes} \geq 2.52312 * 10^{-29}$$

$K = 2^{24},\ L = 2^{12}$:

$$P_{succes} \geq 2.01899 * 10^{-28}$$

Для t таблиць передобчислень маємо:

$$\tilde{P}_{succes} = 1 - (1 - p_{succes})^t$$

При $t = K = 2^{10},$ або ще більше $\tilde{P}_{succes} \to 1$

2. **Приклад виконання атаки: параметри атаки, вхідне 256-бітове повідомлення, його геш-значення, знайдений прообраз, кількість спроб (перевірок різних значень у таблиці передобчислень), яка вам знадобилась, щоб знайти прообраз.**

Застосовано атаку для $K = 2^{20}$ та $L = 2^{10}$, вхідне повідомлення:
01110000111101111110101011111101111101010110011101011110011001011011110111000111111101001110010010101100101110010000010001110010011101110000111110101001001001011110000111101101111000100010001010010010101100110110001010101110011110011101110001010111.
Геш значення: 70BC2CCCDAE2296BDCFAFF9FE5D36376D0A0C3B978CEF1827602D9A6D2A44A3E7FC2A8CC091A8F69
Прообраз: 1D615AB0B9EDC5CFDFD0AAACE38B14E612E63A09D1DF8E019CF5FEE7DD43047D2D84AE5B091A8F69
Кількість перевірок: 22864
Для даного запуску
кількість успіхів: 372
кількість невдач: 99628
Відповідно ймовірність успіху: 0.00372

3. **Результати експериментальних досліджень (у вигляді двох табличок 3x3 із імовірностями успіху атаки при різних значеннях параметрів).**

K\L	2^{10}	2^{11}	2^{12}
2^{20}	0.3%	0.25%	0.2%
2^{22}	0.31%	0.3%	0.275%
2^{24}	0.373%	0.34%	0.32%

При $K = 2^{10}$ побудова такої кількості таблиць є неадекватною задачею, але з такою кількістю таблиць ймовірність успішної атаки прямуватиме до 1, аналогічно для $K = 2^{11}$ та $K = 2^{12}$

4. **Порівняння одержаних результатів між собою і з теоретичними оцінками, висновки:**

Практичні значення виявились значно кращими за теоретичні, при тому запуск другої атаки в силу своєї неймовірності було зупинено після другої години години роботи алгоритму. Основний алгоритм працює довше і відповідно гірше аніж алгоритми пошуку з першого комп'ютерного практикуму. Саме виконання лабораторної було супроводжено моральними та фізичними стражданнями, але ми таке приймаємо адже інакше бути і не могло. Аве радикальня