Міністерство освіти і науки України

Харківський національний університет ім. В. Н. Каразіна

Факультет комп’ютерних наук

Кафедра безпеки інформаційних систем і технологій

Лабораторна робота №7

*з навчальної дисципліни*

«Прикладна криптологія»

Виконав:

Студент групи КБ-31 Кравченко Є. М.

Перевірив:

Професор

Горбенко І. Д.

Старший викладач

Єсіна М. В.

Харків – 2020

**Лабораторна робота №7**

*на тему:*

**«Криптографічні функції гешування»**

**Програма роботи**

1. Вимір швидкості виконання геш-функцій.

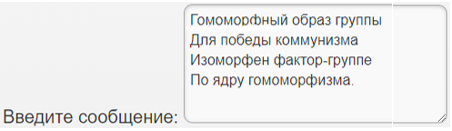
2. Дослідження статистичних властивостей вихідних послідовностей геш-функцій.

**Мета роботи:** ознайомитися з поняттям гешування та його застосуванням у криптографії. Розглянути алгоритми гешування з різними характеристиками та найбільш відомі атаки. У програмному модулі провести демонстрацію функціонування різних геш-функцій. За отриманим результатами провести аналіз функцій гешування та зробити оцінку їх ефективності.

**Хід роботи**

**1. Вимір швидкості виконання геш-функцій.**

Використаємо повідомлення довжиною у 93 символи:



Таблиця 1 — Вимір швидкості виконання геш-функцій

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Геш-функція | Час виконання одного гешування | | | |
| 1 ітерація | 10 ітерацій | 100 ітерацій | 1000 ітерацій |
| BLAKE-256 |  |  |  |  |
| SKEIN-256 |  |  |  |  |
| SHA-256 |  |  |  |  |
| Keccak-256 |  |  |  |  |

За результатами вимірювань видно, що зі збільшенням кількості ітерацій час виконання одного гешування зменшується, при цьому загальний час росте. Найшвидшою геш-функцією можна вважати *BLAKE-256*, а найповільнішою – *Keccak-256*.

**2. Дослідження статистичних властивостей вихідних послідовностей геш-функцій.**

Варіант геш-функції: *SKEIN-256*.

Створюємо 8 різних повідомлень, а значення їх гешів зберігаємо у текстові документи:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |

Таблиця 2 — Результати проходження тестів

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № досліду | Монобітний тест | Тест серій | Кореляційний тест | Тест Поккера |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |

Згенеруємо досить велике геш-значення шляхом додавання усіх раніше використаних геш-значень. Протестуємо отриману послідовність, вибравши довжину 2048 біт.

Результати представлені в гістограмах:

Узагальнимо дані наступним чином:

Як видно з результатів SKEIN-256 пройшов усі тести, окрім кореляційного. Якщо який-небудь з тестів не пройдений, то вважається, що *генератор не пройшов весь комплекс перевірок.*

**Висновки**

Після здійснення досліду функцій гешування, було виявлено, що при збільшенні кількості розрахунків однієї й тієї самої функції час, необхідний на розрахунок однієї функції зменшується. Це пов’язано з тим, що починає працювати кеш-пам’ять.

Протестувавши вихідні послідовності за статистичними тестами для випадкової бітової послідовності, дійшли висновку, що послідовність має властивості випадкової послідовності, але існують кореляційні зв’язки між послідовністю та її циклічними зсувами.

Геш-функція – це перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини.

Лавинний ефект означає, що зміна значення невеликої кількості бітів у вхідному тексті або у ключі веде до «лавинної» зміни значень вихідних бітів шифртексту; це залежність усіх вихідних бітів від кожного вхідного біта.