Исследование криптографических хеш-функций

Выполнил: Макаров Алексей Игоревич, 3 курс 4 группа 2 подгруппа

2024

**Теоритические сведения**

Хеш-функция – математическая или иная функция h = H(М), которая принимает на входе строку символов М, называемую также прообразом, переменной длины n и преобразует ее в выходную строку фиксированной (обычно – меньшей) длины l. Хеширование (или хэширование, англ. hashing) – это преобразование входного массива данных определенного типа и произвольной длины (практически) в выходную битовую строку фиксированной длины. Преобразования называются хеш-функциями, или функциями свертки, а их результаты называют хешем, хеш-кодом, хеш-таблицей или дайджестом сообщения (англ. message digest).

Основные задачи, решаемые с помощью хеш-функций:

• аутентификация (хранение паролей);

• проверка целостности данных;

• защита файлов;

• обнаружение зловредного ПО.

К основным свойствам хеш-функций можно отнести следующие.

Свойство 1. Детерминированность: независимо от того, сколько раз вычисляется H(M), M – const, при использовании одинакового алгоритма код хеш-преобразования h всегда должен быть одинаковым.

Свойство 2. Скорость вычисления хеша h: если процесс вычисления h недостаточно быстрый, система просто не будет эффективной.

Свойство 3. Сложность обратного вычисления: для известного H(М) невозможно (практически) определить М. Это важнейшее свойство хеш-функции для криптографических применений – свойство односторонности преобразования.

Свойство 4. Даже минимальные изменения в хешируемых данных (М ≠ М') должны изменять хеш: Н(M) ≠ Н(М').

Свойство 5. Коллизионная устойчивость (стойкость). Зная М, трудно найти такое М' (М ≠ М'), для которого H(М) = H(М').

Алгоритмы семейства MD-x (2/4/5/6) являются творениями Р. Ривеста; MD – Message Digest. Алгоритм MD6, в отличие от предыдущих версий алгоритма этого семейства, не стандартизован. Алгоритмы семейства SHA (SHA – Secure Hash Algorithm) являются в настоящее время широко распространенными. По существу, во многих случаях завершился переход от SHA-1 к стандартам версии SHA-2. SHA-2 – собирательное название, по сути, аналогами SHA-256 и SHA-512 соответственно.

**Ход работы**

Вариант 8

В данной работе было необходимо реализовывать авторское оконное приложение в соответствии с целью лабораторной работы.

Код программы представлен в листинге 1.

|  |
| --- |
| import hashlib import time   def hash\_message(message: str) -> str:  *"""Функция для хеширования сообщения с использованием SHA-256."""  sha256* = hashlib.sha256()  *sha256*.update(message.encode('utf-8'))  return *sha256*.hexdigest()   def evaluate\_performance(message: str, iterations: int) -> None:  *"""Функция для оценки быстродействия алгоритма хеширования."""  start\_time* = time.time()   for \_ in range(iterations):  hash\_message(message)   *end\_time* = time.time()  *elapsed\_time* = *end\_time* - *start\_time* print(f"Время, затраченное на {iterations} итераций: {  *elapsed\_time*:.6f} секунд")  print(f"Среднее время на итерацию: {*elapsed\_time* / iterations:.6f} секунд")   if \_\_name\_\_ == "\_\_main\_\_":  input\_message = input("Введите сообщение для хеширования: ")  iterations = int(  input("Введите количество итераций для оценки быстродействия: "))   *# Хеширование сообщения* hash\_result = hash\_message(input\_message)  print(f"Хешированное сообщение (SHA-256): {hash\_result}")   *# Оценка быстродействия* evaluate\_performance(input\_message, iterations) |

Листинг 1 – Программная реализация приложения

Результат работы программы представлен в листинге 2:

|  |
| --- |
| ❯ python3 lab11\_ib.py  Введите сообщение для хеширования: helo  Введите количество итераций для оценки быстродействия: 10000  Хешированное сообщение (SHA-256): f4e454f802b88d2f64168ff1742e8cf413fd677d38b87cbefb45821f8981b912  Время, затраченное на 10000 итераций: 0.012135 секунд  Среднее время на итерацию: 0.000001 секунд  : 0.00012683868408203125 секунд |

Листинг 2 – Результат работы приложения

**Вывод**: таким образом, были закреплены теоретические знания по алгебраическому описанию и алгоритмам реализации операций вычисления однонаправленных хеш-функций.