Санкт-Петербургский Национальный Исследовательский Университет

Информационных Технологий, Механики и Оптики

Факультет инфокоммуникационных технологий

Лабораторная работа №2

Вариант № 5

Выполнили:

Конопля Алексей, Комелин Глеб

Проверил:

Мусаев А.А.

Санкт-Петербург

2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Данная лабораторная работа посвящена изучению алгоритмов хэширования.

ПОСТАНОВКА ЗАДАЧИ

Реализовать алгоритм хэширующий строку, вводимую пользователем, с помощью алгоритмов: хэширования делением, CRC32.

ХОД РАБОТЫ

Хеширование – метод адресации данных для быстрого поиска по ключевым выражениям.

Метод деления.

Данный метод использует следующую формулу расчёта хэша:

$$h(m) = k \bmod m$$

где k – ключ хэширования m – размер массива.

Плюсы метода:

1. Простота реализации
2. Скорость работы

Минусы метода:

1. Большой шанс коллизии
2. Сложность выбора ключа

Результат выполнения программы

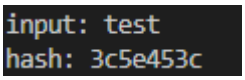

Рисунок 1. Результат выполнения метода деления

CRC-32

Данный метод применяется для защиты данных и обнаружения ошибок в потоке информации.

Для вычисления полинома, представляющего собой входные данные используют следующую формулу:

$$P(x) = \sum_{n=0}^{N-1} a_n x^n$$

Так последовательность 111010 преобразуется в полином вида.

$$P(x) = 1 * x^5 + 1 * x^4 + 1 * x^3 + 0 * x^2 + 1 * x^1 + 0 * x^0$$

Значение CRC получается по следующей формуле

$$R(x) = P(x) * x^N mod\ G(x)$$

где R(x) – контрольная сумма в двоичном виде

P(x) – многочлен входных данных

G(x) – порождающий многочлен

Результат выполнения программы

```
input: test
hash 749d77bb
```

Рисунок 2. Результат выполнения метода CRC-32

ЗАКЛЮЧЕНИЕ

В ходе выполнения лабораторной работы были изучены и реализованы методы: деления и CRC-32.

ПРИЛОЖЕНИЯ

Приложение А.

https://github.com/AlexeyKonoplia/lab2