Санкт-Петербургский Национальный Исследовательский Университет

Информационных Технологий, Механики и Оптики

Факультет Инфокоммуникационных Технологий

**Домашнее задание 2. Алгоритмы Хеширования**

**Вариант №9**

Выполнил

Абдалла Мустафа Абдалла Мохамед Ахмед

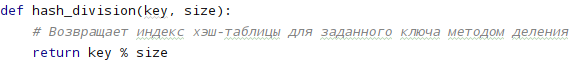
Проверил

Мусаев А. А.

Санкт-Петербург, 2023

Введение

Хэширование по методу деления — это один из простых способов генерации хеш-кодов для данных. Алгоритм этого метода заключается в том, чтобы разделить значение на некоторую константу и использовать остаток от деления как хеш-код. Ниже приведена алгоритм программы хэширования метод деления на языке *Python* без использование дополнительные библиотеки.



В этом коде функция *hash\_division* принимает два параметра: *key* (ключ) и *size* (размер хэш-таблицы). Она возвращает индекс хэш-таблицы для заданного ключа, который получается путем взятия остатка от деления ключа на размер хэш-таблицы.

Пример использования этой функции:

Изображение выглядит как текст

Автоматически созданное описание

В этом примере мы создаем хэш-таблицу из 10 элементов и заполняем ее ключами, используя функцию *hash\_division* для вычисления индексов. Результатом будет следующий список ключей:



Как видно из примера, ключи были сохранены в соответствующих ячейках хэш-таблицы. Если бы мы хотели получить значение для ключа, мы бы использовали тот же алгоритм для вычисления индекса и затем получили бы значение из соответствующей ячейки хэш-таблицы.

Хеширование методом MD5

Хеширование - это процесс преобразования произвольного входного сообщения (данных) фиксированной длины, которое называется хэш-значением. Хэширование используется для безопасного хранения паролей, цифровых подписей и проверки целостности данных. Одним из самых распространенных методов хеширования является метод md5, который был разработан в 1991 году Рональдом Ривесом. Он является одним из наиболее широко используемых алгоритмов хэширования, который обеспечивает надежную защиту от подделки и изменения данных. В этом методе сообщение разбивается на блоки и подвергается серии математических операций, которые и определяют хэш-значение. Одним из основных преимуществ метода md5 является его скорость и эффективность, что делает его особенно полезным в ситуациях, где требуется быстрое хэширование больших объемов данных.

Изображение выглядит как текст

Автоматически созданное описание

Заключение

Результатом выполнения задания стал полноценный рабочий код алгоритма хэширования методами деления и MD5 на Python, который можно использовать для вычисления хэш-значений для произвольных сообщений.

Я считаю, что выполнение данного задания было очень полезным для моего обучения и позволило мне улучшить свои знания и навыки в области криптографии и программирования.

Список используемых источников

Код, используемый в работе, ссылка на GitHub: <https://github.com/Mostafa182003/alg1>