

Лабораторная работа 3.

Исследование хеш-функций с различными вводными условиями.

Требования задания

ель рабо ы – расшифровать набор данных, зашифрованный с помощью хеш-функции с использованием модификатора входа – соли, а также проанализировать решение аналогичной задачи при различных условиях.

Порядок выполнения лабораторной работы:

1. Изучить особенности шифрования телефонных номеров.
2. Написать программу для деобезличивания датасета.
3. Протестировать программу на выданном варианте.
4. Протестировать с еще минимум **3-мя различными хеш-функциями** (1 алгоритм на 1 семейство), которыми зашифрован исходный деобезличенный набор.
5. Написать от чего меняется скорость расшифровки. **Влияние вида соли, длины соли и хеш-функции на скорость расшифровки датасета.** А так же ответить на вопрос – сколько нужно знать телефонов из предложенного датасета, чтоб 100% его взломать?
6. Написать отчет.

Вариантов всего 10. Поэтому, берем вариант из таблиц на 2 и 3 странице.

Содержание отчета

1. Цель работы.
2. Краткое описание хеш-функций, техники взлома **Brute force** и понятия “Соли” на основании лекционно-практического материала.
3. Представить описание схемы пошагового выполнения алгоритма.
4. Формализация задачи, представление программы на выбранном вами языке, спецификация программы, раскрывающая смысл работы алгоритма.
5. Описание контрольного примера.
6. Анализ результатов работы алгоритма и вводных условий.

7. Выводы по работе.

[illegible]

[illegible]