Лабораторная работа 3.

Исследование хеш-функций с различными вводными условиями.

**Требования задания**

*Цель работы* – 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.

|  |  |
| --- | --- |
| Группа 215 | |
| ФИО | Вариант |
| Абрахин Егор Дмитриевич st117271@student.spbu.ru | 1 |
| Антонян Арсений Антонович st117248@student.spbu.ru | 2 |
| Аршинов Артём Викторович st117273@student.spbu.ru | 3 |
| Багров Владимир Алексеевич st117262@student.spbu.ru | 4 |
| Бек Вячеслав Александрович st117260@student.spbu.ru | 5 |
| Беляева Ася Павловна st117245@student.spbu.ru | 6 |
| Голуб Глеб Ярославович st117275@student.spbu.ru | 7 |
| Киселев Михаил Васильевич st117281@student.spbu.ru | 8 |
| Кубянин Никита | 9 |
| Лихошерстова Ксения Андреевна st095261@student.spbu.ru | 10 |
| Марков Семён Николаевич st117246@student.spbu.ru | 1 |
| Махаев Роман Владимирович st117255@student.spbu.ru | 2 |
| Овчинников Святослав Александрович st117252@student.spbu.ru | 3 |
| Петрова Екатерина Дмитриевнаst117276@student.spbu.ru | 4 |
| Рылова Александра Игоревна st117013@student.spbu.ru | 5 |
| Сергеев Дмитрий Юрьевич st117243@student.spbu.ru | 6 |
| Сериков Кирилл Геннадьевич st117257@student.spbu.ru | 7 |
| Скорынин Павел Алексеевич st117244@student.spbu.ru | 8 |
| Сурин Игнат Сергеевич st117266@student.spbu.ru | 9 |
| Трофимов Иван Александрович st117263@student.spbu.ru | 10 |
| Черевко Максим Евгеньевич st117272@student.spbu.ru | 1 |

|  |  |
| --- | --- |
| Группа 216 | |
| ФИО | Вариант |
| Аникин Роман Сергеевич st116634@student.spbu.ru | 1 |
| Асташенкова Милана Константиновна st117259@student.spbu.ru | 2 |
| Барафанов Артём Александрович st117258@student.spbu.ru | 3 |
| Бурганова Рената Максимовна st117269@student.spbu.ru | 4 |
| Горынцев Роман Николаевич st117251@student.spbu.ru | 5 |
| Дегтярёв Евгений Андреевич st096467@student.spbu.ru | 6 |
| Добрынин Даниил | 7 |
| Зайнуллин Мансур Альбертович st107049@student.spbu.ru | 8 |
| Ильютчик Илья Сергеевич st116034@student.spbu.ru | 9 |
| Кривошеин Алексей Евгеньевич st117264@student.spbu.ru | 10 |
| Крылов Александр Сергеевич st117277@student.spbu.ru | 1 |
| Масгутов Михаил Александрович st117274@student.spbu.ru | 2 |
| Осадчев Тимофей Владимирович st117256@student.spbu.ru | 3 |
| Полугрудов Артём Александрович st117270@student.spbu.ru | 4 |
| Пушкарев Никита Павлович st117247@student.spbu.ru | 5 |
| Пчелкова Анна st116032@student.spbu.ru | 6 |
| Рыбин Евгений Дмитриевич st077361@student.spbu.ru | 7 |
| Седегова Дарья Павловна st117265@student.spbu.ru | 8 |
| Сергеева Александра Алексеевна st117268@student.spbu.ru | 9 |
| Скрипников Владислав st116031@student.spbu.ru | 1 |
| Сон Максим Петрович st117250@student.spbu.ru | 1 |
| Сулимов Андрей Станиславович st117261@student.spbu.ru | 2 |
| Уманец Олег st116029@student.spbu.ru | 3 |
| Шарабарин Михаил st122304@student.spbu.ru | 4 |
| Шведов Сергей Павлович st116036@student.spbu.ru | 5 |
| Юдинцев Степан Алексеевич st117249@student.spbu.ru | 6 |
| Паршанов Георгий | 7 |