**МИНОБРНАУКИ РОССИИ**

**САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**КАФЕДРА КОМПЬЮТЕРНОГО МОДЕЛИРОВАНИЯ И МНОГОПРОЦЕССОРНЫХ СИСТЕМ**

**ОТЧЕТ**

**по лабораторной работе**

**по дисциплине “Алгоритмы и структуры данных”**

**на тему “Деобезличивание данных”,**

**вариант 11**

|  |  |
| --- | --- |
| Студент | Михайлов И. С. |
| Преподаватель | Щеголева Н. Л. |

Санкт-Петербург

2022 г.

**Оглавление:**

[Цель работы](#_35ppp6dgsf4p)

[Задача](#_l20wsasujrtf)

[Теоретическая часть](#_odxixc4encsn)

[Алгоритм метода](#_vkx9fl7mxe6n)

[Контрольный пример](#_pfgfquw8nhdn)

[Вывод](#_laztutv55ct2)

# Цель работы

Взломать шифр входящей базы данных

# Задача

Получить информацию из зашифрованных различными способами полей таблицы

# Теоретическая часть

В исходной таблице 3 столбца, в них находится информация о номере телефона, электронной почте и адресе проживания соответственно. Визуально было определено, что в первом столбце данные были зашифрованы хэш-функцией sha1, а во втором и третьем столбце - шифром Цезаря. В дальшем эти наблюдения подтвердились.

# Алгоритм метода

В первом столбце хэш-функция была расшифрована программой hashcat. Задачу облегчила информация о том, что в этом столбце находится именно номер телефона. Передача аргумента ?d?d?d?d?d?d?d?d?d?d?d уточнила, что данные в ячейках состоят из 11 цифр. Благодаря этому данный шаг был выполнен за измеримое время. Hashcat выдает пары - исходное значение и его хэш. Но их порядок произвольный, поэтому при заполнении таблицы алгоритм ищет в результате hashcat нужный хэш и записывает его исходное значение из пары.

Во втором и третьем столбцах используется шифр Цезаря, который применен только к буквам. Разгадывается он перебором всех возможных сдвигов. Для почты, которая записана латиницей количество всех вариантов - 26, а для адреса, записанного кириллицей - 32 (Буква ‘Ё’ не используется и пропускается при сдвиге). Чтобы понять, что данный сдвиг является правильным нужно проверить полученный с помощью него текст на содержание одной из необходимых подстрок. В случае с почтой это окончания адресов почтовых сервисов:

* .com
* .org
* .net
* .biz
* .info

А для адреса достаточно одной подстроки “кв.”.

Также в таблицу записываются сдвиги относительно исходной зашифрованной таблицы: в четвертый столбец сдвиги второго столбца и в пятый столбец сдвиги третьего столбца.

# Контрольный пример



Рис. 1. Пример расшифрованной таблицы

# Вывод

В ходе данной работы были исследованы и изучены методы шифрования данных, а также способы их дешифрования. Эти способы были применены на практике для взлома базы данных, зашифрованной с помощью sha1 и шифра Цезаря.