Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Кафедра автоматизированных систем управления (АСУ)

Шифр сдвига

Лабораторная работа №1

по дисциплине

«Информационная безопасность»

Студент гр. 430-2

_____А.А. Лузинсан

«_____»_____2023 г.

Руководитель

Профессор кафедры АСУ, д.т.н.

_____ А.Н. Горитов

«____»_____2023 г.

Томск 2023

Оглавление

Введение

Цель: познакомиться и научиться работать с алгоритмами донаучной криптографии.

Задание по варианту №2: напишите программу, позволяющую зашифровать и расшифровать сообщения с использованием шифра сдвига. Входные и выходные данные запишите в файл типа .txt.

1 ХОД РАБОТЫ

Шифр сдвига, иначе известный как код Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиции левее или правее него в алфавите.

Например, имеется исходный текст: АБВГДЕЖЗ.

В шифре со сдвигом вправо на 3, зашифрованный текст будет иметь вид: ГДЕЖЗИЙК.

В реализации алгоритма использовались списки алфавитов кириллицы и латиницы в обоих регистрах, для того чтобы поддерживался сдвиг для буквенных обозначений. Во всех остальных случаях алгоритм ориентируется на кодовое обозначение символа и сдвигает его значение на количество позиций, указанное пользователем. Однако при такой реализации однозначное шифрование гарантируется только для буквенных обозначений, тогда как остальные символы могут выйти в область кодов буквенных символов, что не даёт декодировать полученное сообщение.

Основная функция, реализующая шифр сдвига, представлена в листинге 1.1. Алгоритм проходится в цикле по символам кодируемой строки и фиксирует, какому алфавиту принадлежит рассматриваемый символ. Далее определяется нормированное значение сдвига на случай непреднамеренной (или преднамеренной) ошибки пользователя, то есть обрабатывается случай, когда пользователь указал значение сдвига большее, чем мощность самого алфавита. И наконец инициализируется индекс нового символа в текущем алфавите для рассматриваемого алфавита. В случае, если рассматриваемый символ не является буквой, берётся код символа и это значение суммируется со сдвигом, а далее возвращается сам символ.

Алгоритмом обеспечивается как положительный, так и отрицательный сдвиг.

Листинг 1.1 — Определение функции кодирования строки

```
def encrypting_row(row, shift):
    cyrillic_lower = [chr(symbol) for symbol in range(ord('а'), ord('я') + 1)]
    cyrillic = [chr(symbol) for symbol in range(ord('А'), ord('Я') + 1)]
    latin_lower = [chr(symbol) for symbol in range(ord('a'), ord('z') + 1)]
    latin = [chr(symbol) for symbol in range(ord('A'), ord('Z') + 1)]
    sign = -1 if shift < 0 else 1
    shift = abs(shift)
    enc_row = []
    for symbol in row:
        if symbol in cyrillic_lower + cyrillic + latin_lower + latin:
            if symbol in cyrillic_lower:
                alphabetic = cyrillic_lower
            elif symbol in cyrillic:
                alphabetic = cyrillic
            elif symbol in latin_lower:
                alphabetic = latin_lower
            elif symbol in latin:
                alphabetic = latin
            shift_for_symbol = (shift % (len(alphabetic) - 1)) * sign
            index = (alphabetic.index(symbol) + shift_for_symbol) % (len(alphabetic))
            enc_row.append(alphabetic[index])
        else:
            enc_row.append(chr(ord(symbol) + (shift * sign)))
    return enc_row
```

2 ТЕСТИРОВАНИЕ

Программа поддерживает файловый ввод исходного текста, либо же ввод вручную, а также вывод результата в выходной файл output.txt. Результат работы для файлового ввода представлен на рисунке 2.1.

Пример работы программы на данных, введённых вручную, представлен на рисунке 2.2.

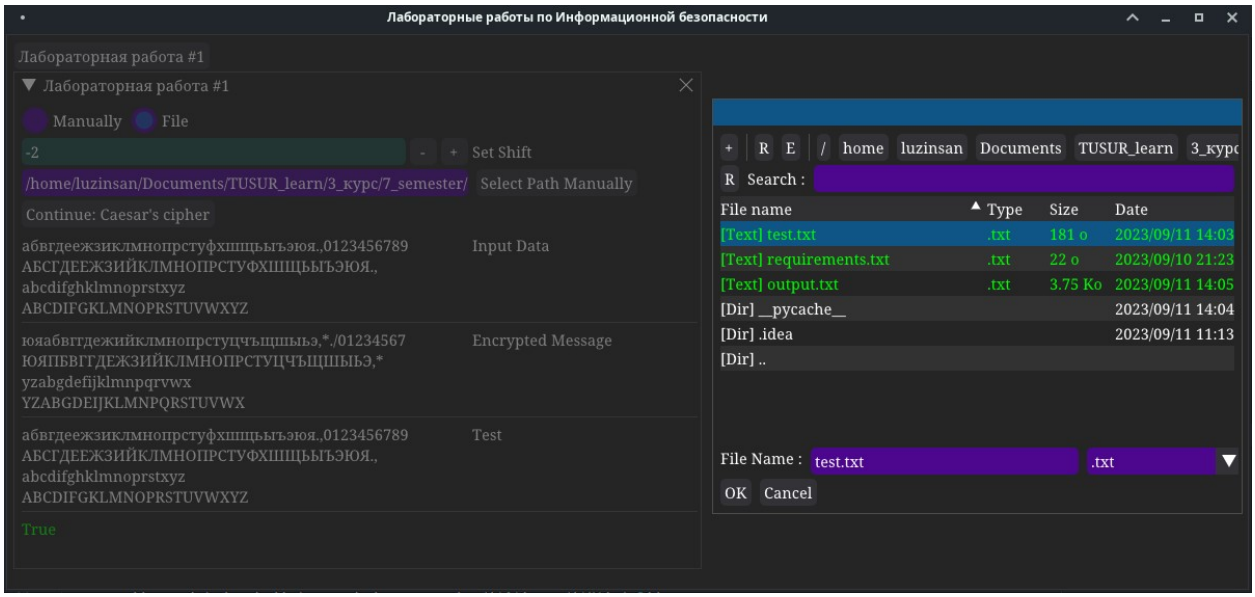

Рисунок 2.1 — Кодирование текста из файла

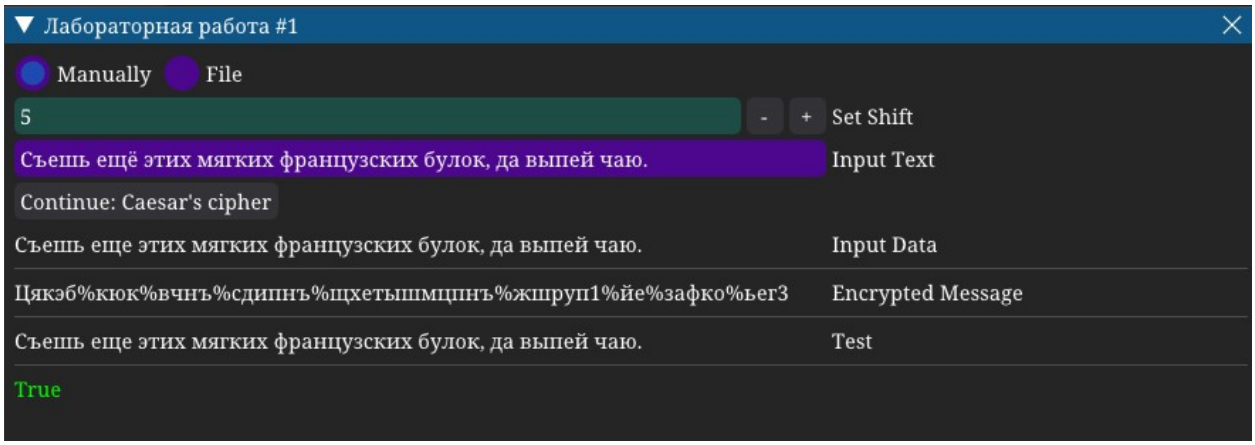

Рисунок 2.2 — Кодирование текста, введённого вручную

Заключение

В результате выполнения лабораторной работы я познакомилась и научилась работать с алгоритмом донаучной криптографии на примере шифра сдвига, а также выполнила задание в соответствие с заданным вариантом на языке Python.