Лабораторная работа №2

Математические основы защиты информации и информационной безопасности

Колчева Юлия Вячеславовна

Содержание

# Цель работы

Изучить шифры перестановки, реализовать программным путём маршрутное шифрование, шифрование с помощью решёток и таблицу Виженера.

# Задание

1. Реализовать маршрутное шифрование
2. Реализовать шифрование с помощью решёток
3. Реализовать шифрование с помощью таблицы Виженера

# Выполнение лабораторной работы

Так как я не изучала язык Julia на бакалавриате, лабораторную работу я реализовала на python. При дальнейшем изучении я перейду на новый язык.

Для реализации маршрутного шифрования мной была написана следующая программа (рис. 1 ) :

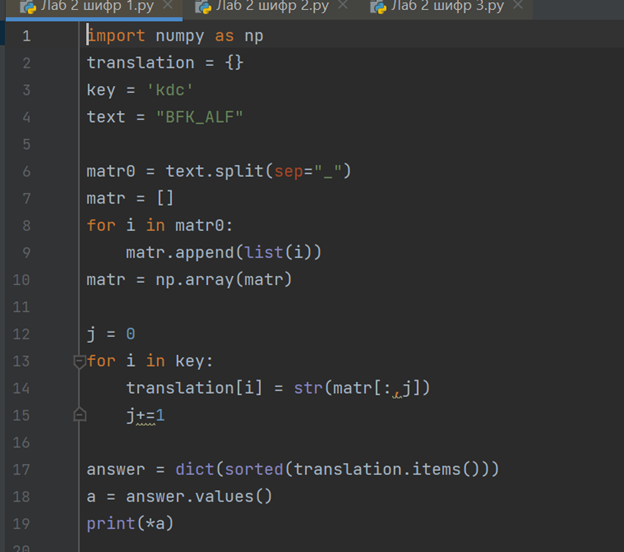


Figure 1: Программа реализации первого шифра

В данной программе:

2-3 строки: инициализация используемых переменных

6-10 строка: деление заданного текста на части и запись в матрицу

12-15: заполнение “переводчика” , каждой букве пароля присваевается соответсвующий столбец матрицы

Далее представлен результат работы программы (рис. 2 )

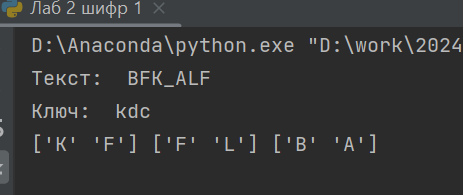


Figure 2: Вывод программы

Как видно, программа работает верно

Теперь представим программу шифрования с помощью решёток (рис. 3 ) (рис. 4 )

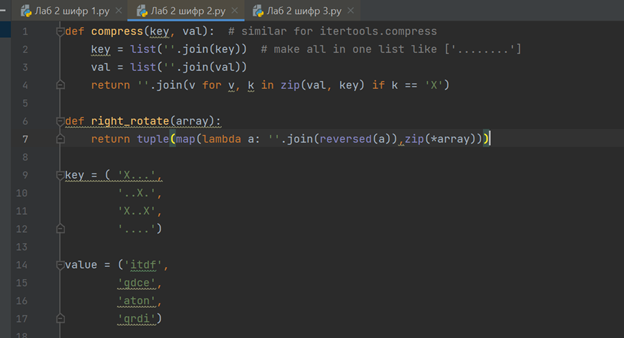


Figure 3: Реализация второго шифра 1

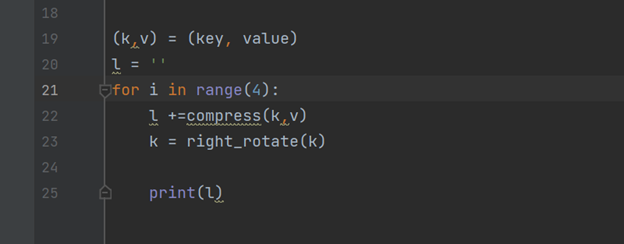


Figure 4: Реализация второго шифра 2

В данной программе:

1-4 строки: реализация “прикладывания” решётки к имеющейся матрице

6-7 строка: “переворот” матрицы на 90 градусов

9-12: заданная “решётка”

14-17: матрица букв

19: сокращённая запись

21-23: запуск функций

Посмотрим на результат работы программы, на ней представлены все повороты решёток и конечный шифр (рис. 5 )

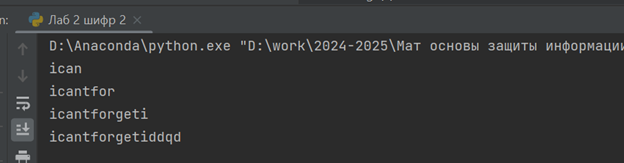


Figure 5: Вывод программы

Программа работает верно.

Реализуем последний шифр - таблицу Виженера (рис. 6 ) (рис. 7 ) (рис. 8 )

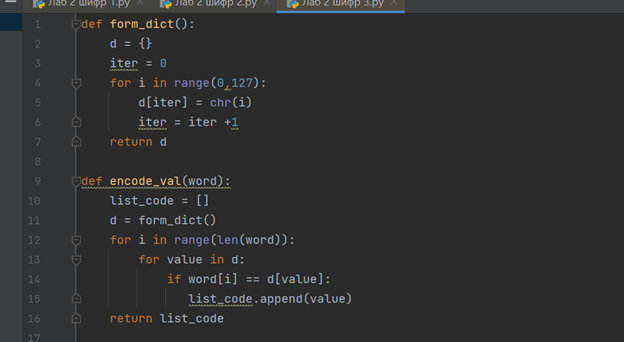


Figure 6: Реализация третьего шифра 1

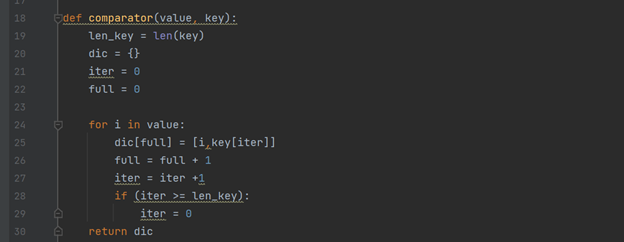


Figure 7: Реализация третьего шифра 2

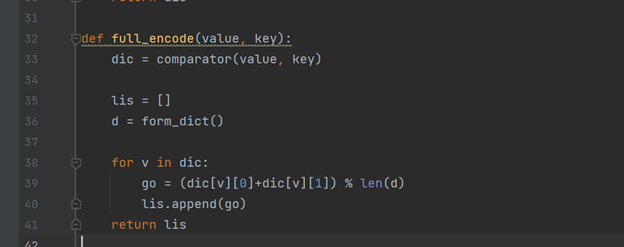


Figure 8: Реализация третьего шифра 3



Figure 9: Реализация третьего шифра 4

В данной программе:

1-7: функция задающая индексы значений, которые мы будем использовать

9-16: функция, сопоставляющая значения индексов в тексте

18-22: сдвиг по значениям индексов

Последнее изображение (рис. 9 ) задаёт текст, ключ и запускает функции программы.

Результаты работы программы (рис. 10 )

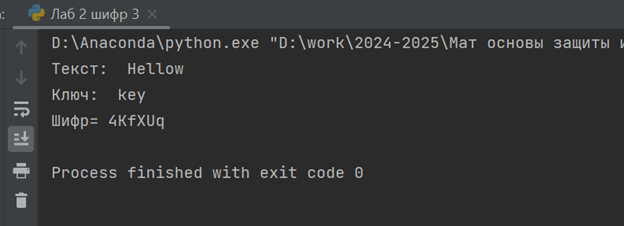


Figure 10: Вывод программы

# Выводы

Изучила шифры перестановки, реализовала программным путём маршрутное шифрование, шифрование с помощью решёток и таблицу Виженера.

# Список литературы

Лабораторная работа №2

Шифры перестановки [Электронный ресурс]. URL: https://esystem.rudn.ru/mod/folder/view.php?id=1150970