Лабораторная работа №1

Математические основы защиты информации и информационной безопасности

Колчева Юлия Вячеславовна

Содержание

# Цель работы

Изучить шифр Цезаря и шифр Атбаш, научиться реализации данных шифров программным путём.

# Задание

1. Реализовать шифр Цезаря с произвольным ключом k
2. Реализовать шифр Атбаш

# Выполнение лабораторной работы

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

Для реализации шифра Цезаря мной была написана следующая программа:

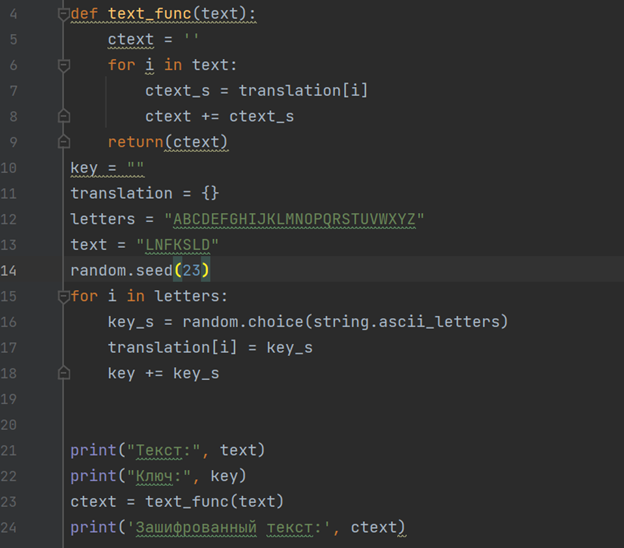


Figure 1: Программа реализации шифра Цезаря

В данной программе:

4-9 строки: функция, реализующая “перевод” текста в шифртекст побуквенно

10 строка: создание пустого словаря

11: зададим алфавит, который будем кодировать. Можно использовать юникод, однако тогда в шифре мы можем получить не только буквы, но и знаки.

12: текст, который будем кодировать

14: Задаем корень, чтобы ключ каждый запуск оставался одинаковым

15-18: формирование случайного ключа и запись в словарь посимвольное соответствие.

23: запуск функции

Далее представлен результат работы программы

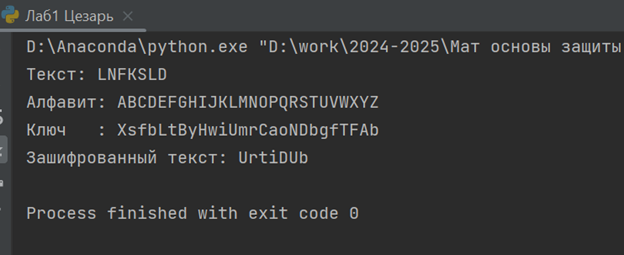


Figure 2: Вывод программы

Как видно, программа работает верно

Теперь представим программу реализации шифра Атбаш

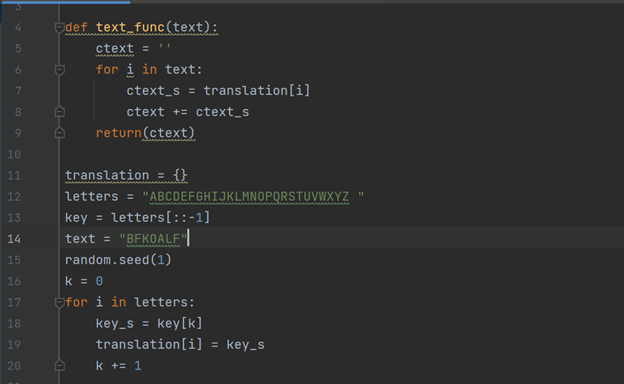


Figure 3: Реализация шифра Атбаш 1

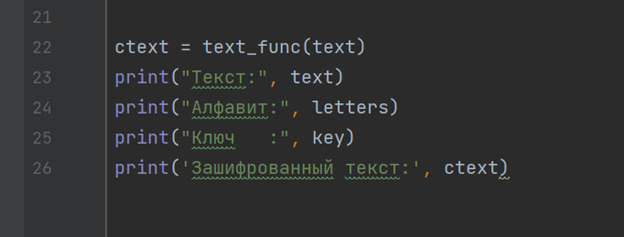


Figure 4: Реализация шифра Атбаш 2

В данной программе:

4-9 строки: функция, реализующая “перевод” текста в шифртекст побуквенно

11 строка: создание пустого словаря

12: зададим алфавит, который будем кодировать.

13: В данном случае ключом будет являться наш же алфавит в обратном порядке (с пробелом)

17-20: запись в словарь посимвольное соответствие.

22: запуск функции

Посмотрим на результат работы программы

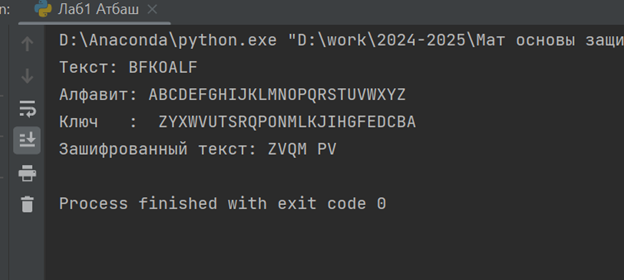


Figure 5: Вывод программы

Программа работает верно.

# Выводы

Я изучила шифр Цезаря и шифр Атбаш, научилась реализации данных шифров программным путём.

# Список литературы

Лабораторная работа №1 Шифры простой замены [Электронный ресурс]. URL: https://esystem.rudn.ru/pluginfile.php/2368411/mod\_folder/content/0/lab01.pdf?forcedownload=1