Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Гисматуллин Артём Вадимович НПИбд-01-22

Содержание

[1 Цель работы 1](#__RefHeading___Toc197_3146060361)

[2 Задание 1](#__RefHeading___Toc199_3146060361)

[3 Выполнение лабораторной работы 1](#__RefHeading___Toc201_3146060361)

[4 Выводы 3](#__RefHeading___Toc203_3146060361)

[Список литературы 3](#__RefHeading___Toc205_3146060361)

# 1 Цель работы

* Освоить на практике применение режима однократного гаммирования

# 2 Задание

Последовательно выполнять все пункты, занося ответы и замечания в отчет.

# 3 Выполнение лабораторной работы

1. Пропишем две функции на языке Python, где у нас будет находится приложение-шифратор-дешифратор. Функция main получает на вход данные о строке, файлах и отправляет в функцию xor\_script, где производится операция XOR  каждым символом из файла filename и строкой s. Если символов в файле больше, чем в строке s, то строка сдвигается влево на один символ. Результат записывается в файл outfilename (рис. 1)

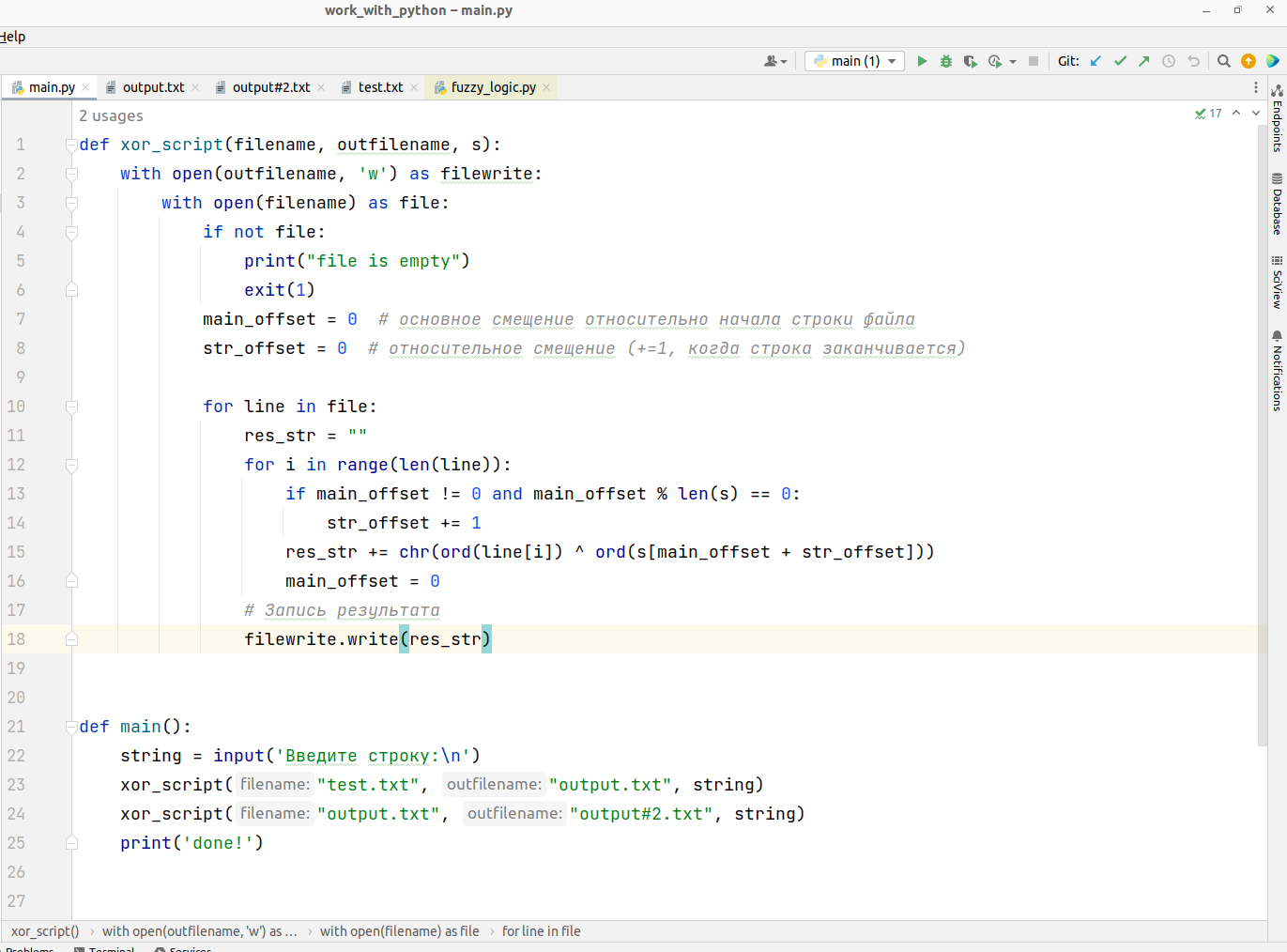


Рис. 1: Интерпретатор. Код программы

1. Получаем следующий вывод (названия файлов выделены) (рис. 2)

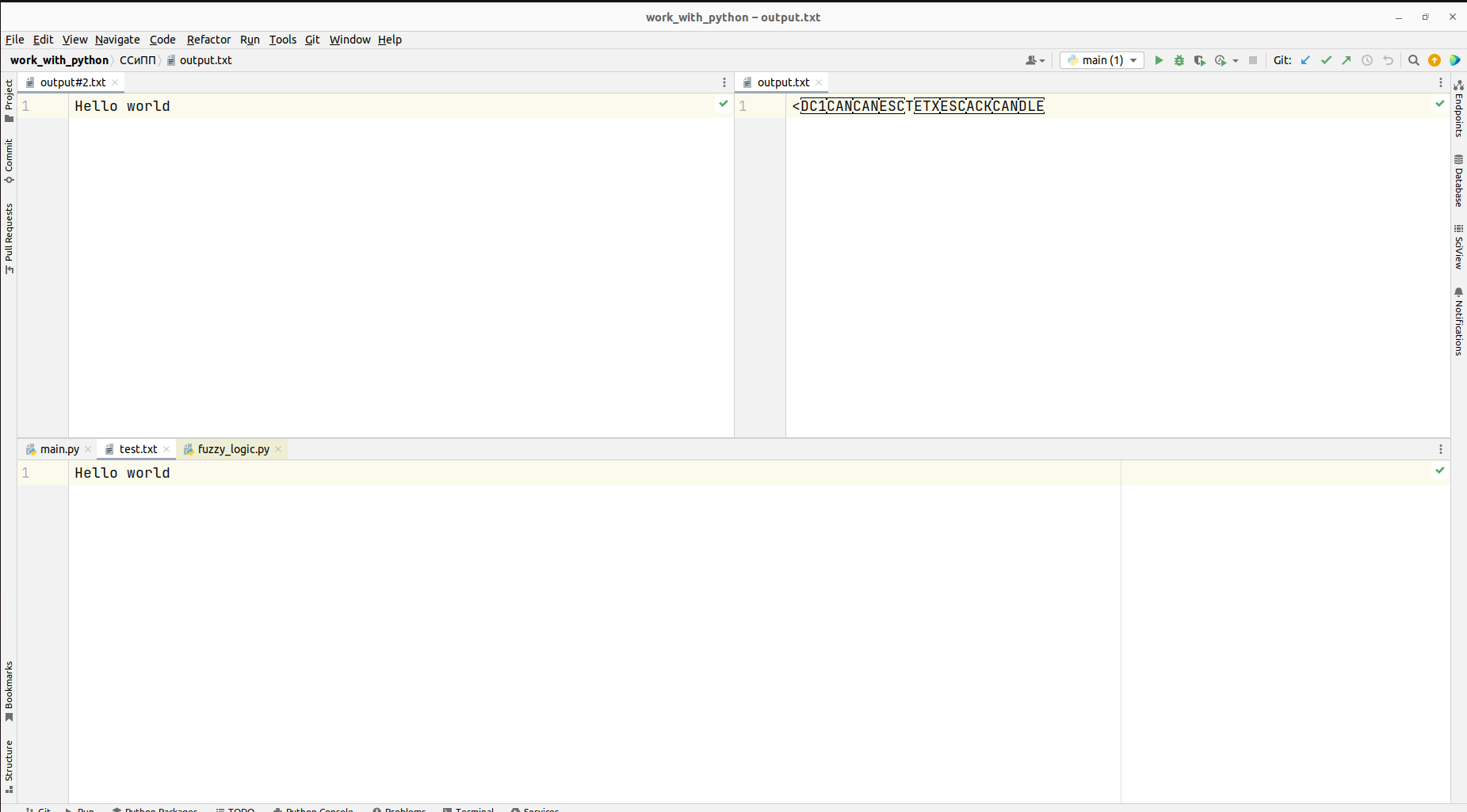


Рис. 2: Интерпретатор. Результат работы

# 4 Выводы

В ходе выполнения данной лабораторной работы были освоены на практике методы однократного гаммирования

# Список литературы

1. [Шифрование методом гаммирования](http://altaev-aa.narod.ru/security/XOR.html)
2. [Режим гаммирования в облочном алгоритме шифрования](https://kabinfo.ucoz.ru/index/shifr_reshetka_kardano/0-374)