Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Гисматуллин Артём Вадимович НПИбд-01-22

Содержание

Список иллюстраций

Список таблиц

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. 3.1)

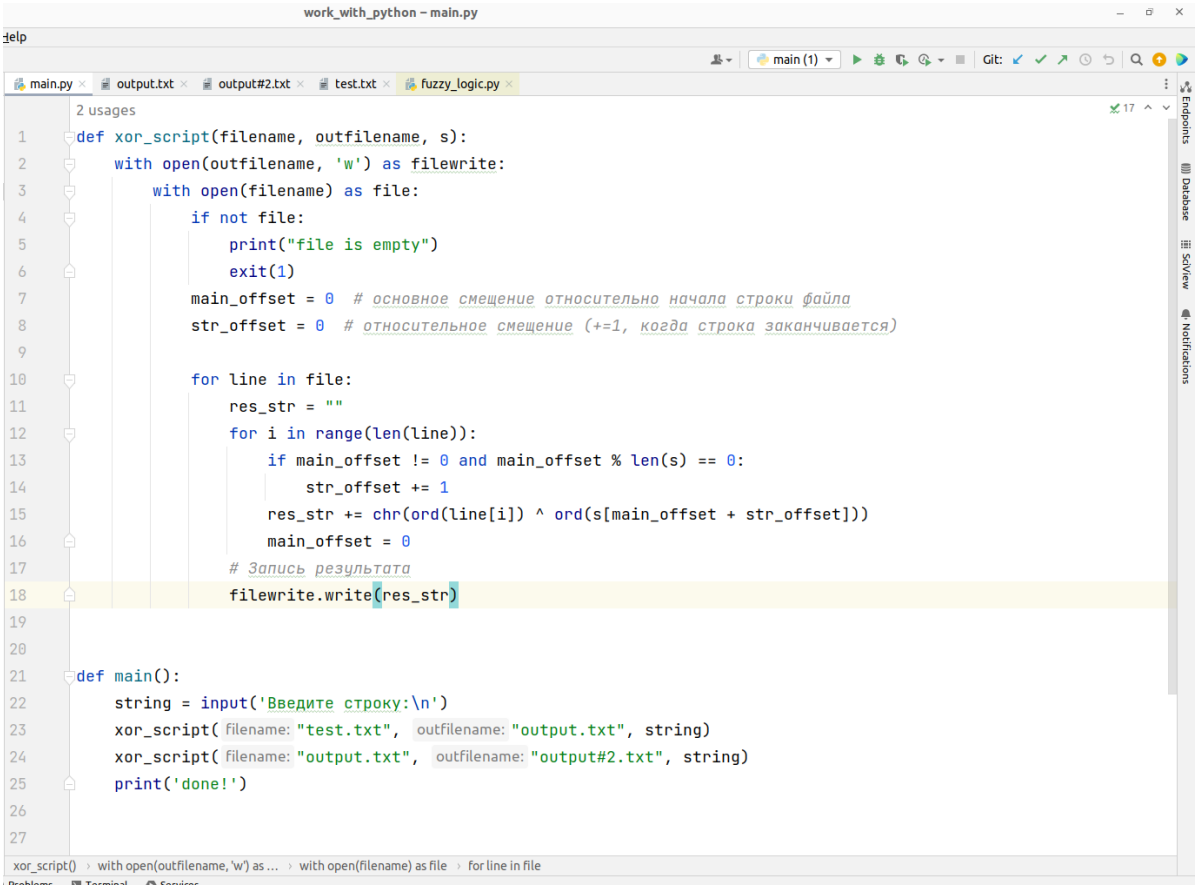

Рис. 3.1: Интерпретатор. Код программы

2. Получаем следующий вывод (названия файлов выделены) (рис. 3.2)

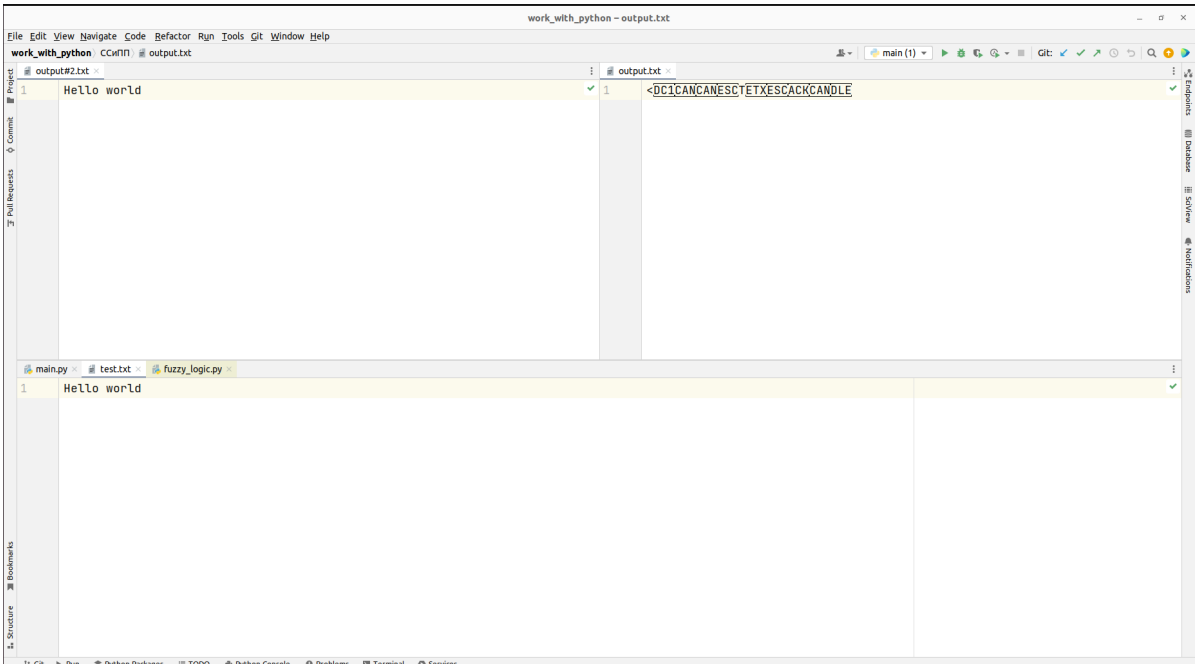

Рис. 3.2: Интерпретатор. Результат работы

4 Выводы

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

Список литературы

1. Шифрование методом гаммирования
2. Режим гаммирования в облочном алгоритме шифрования