

Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Гисматуллин Артём Вадимович НПИбд-01-22

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	10
	Список литературы	11

Список иллюстраций

3.1	Интерпретатор. Код программы	8
3.2	Интерпретатор. Результат работы	9

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 находиться 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)

The screenshot shows a Python IDE window titled "work_with_python - main.py". The editor displays a Python script with the following code:

```
1 def xor_script(filename, outfilename, s):
2     with open(outfilename, 'w') as filewrite:
3         with open(filename) as file:
4             if not file:
5                 print("file is empty")
6                 exit(1)
7             main_offset = 0 # основное смещение относительно начала строки файла
8             str_offset = 0 # относительное смещение (+1, когда строка заканчивается)
9
10            for line in file:
11                res_str = ""
12                for i in range(len(line)):
13                    if main_offset != 0 and main_offset % len(s) == 0:
14                        str_offset += 1
15                    res_str += chr(ord(line[i]) ^ ord(s[main_offset + str_offset]))
16                    main_offset = 0
17                # Запись результата
18                filewrite.write(res_str)
19
20
21 def main():
22     string = input('Введите строку:\n')
23     xor_script(filename="test.txt", outfilename="output.txt", string)
24     xor_script(filename="output.txt", outfilename="output#2.txt", string)
25     print('done!')
```

The code implements a XOR cipher. The `xor_script` function takes a filename, an outfilename, and a string `s` as arguments. It opens the outfilename in write mode and the filename in read mode. If the file is empty, it prints "file is empty" and exits. It then iterates over each line in the file, applying a XOR operation between the line's characters and the characters in `s` (rotated by `main_offset`). The result is stored in `res_str` and written to the outfilename. The `main` function prompts the user for a string and calls `xor_script` twice with different filenames and the same string.

Рис. 3.1: Интерпретатор. Код программы

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

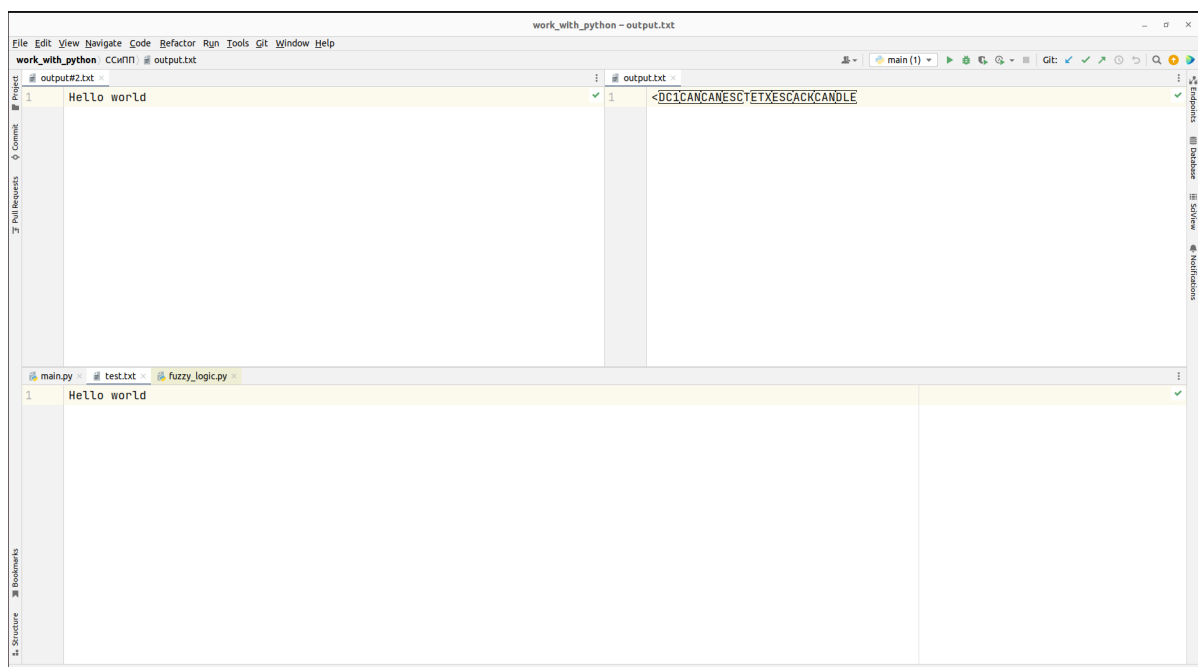


Рис. 3.2: Интерпретатор. Результат работы

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 блочном алгоритме шифрования