

Отчет по лабораторной работе номер 8

Хамбалеев Булат Галимович

Содержание

1	Цель работы	5
2	Задание	6
3	Теория	7
4	Выполнение работы	8
5	Библиография	9
6	Выводы	10

List of Tables

List of Figures

4.1 рис.1. Программа, часть 1. 8

1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

2 Задание

Лабораторная работа подразумевает использование языков программирования для создания программы для шифрования и дешифрования в режиме однократного гаммирования при известном ключе.

3 Теория

Гаммирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных.

4 Выполнение работы

1. Разработаем приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования и расшифруем два текста, зная только один из них и не зная ключа.(рис 1-2)

```
import string
import random

string1='НаВашисходящийот1204'

string2='ВСеверныйфилиалБанка'

def generator(length,abc):
    return ''.join(random.choice(abc)for i in range(length))

abc=string.ascii_letters.join(string.digits)

key=generator(len(string1),abc)

def gamm(string,key):
    return ''.join(chr(n^m) for n,m in zip ([ord(i) for i in string],[ord(i) for i in key]))

a1=gamm(string1,key)

a2=gamm(string2,key)

a=gamm(a1,a2)

gamm(a,string1)

'ВСеверныйфилиалБанка'

gamm(a,string2)

'НаВашисходящийот1204'
```

Figure 4.1: рис.1. Программа, часть 1.

5 Библиография

1. ТУИС РУДН

2. Статъа на сайте "<https://ru.wikipedia.org/wiki/%D0%93%D0%B0%D0%BC%D0%BC%D0%B8>

6 Выводы

Во время выполнения лабораторной работы я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.