

Отчет по лабораторной работе номер 3

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. Гамма.	8
4.2	рис.2. Гаммирование в действии.	8

1 Цель работы

Реализовать алгоритм шифрования гаммированием конечной гаммой.

2 Задание

Задание подразумевает реализацию алгоритма шифрования гаммированием коненой гаммой на языке программирования Python.

3 Теория

Гаммирование – метод последовательного симметричного шифрования, суть которого состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, которая называется гаммой.

4 Выполнение работы

1. Реализуем класс Gamms шифрования гаммированием.(рис. 1)

```
Ввод [78]: class Gamma():  
  
    def __init__(self, key):  
        self.abc = 'АБВГДЕЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ'  
        self.key = [self.abc.find(k)+1 % 33 for k in key.upper()]  
  
    def code(self, word):  
        digits = [self.abc.find(k)+1 for k in word.upper()]  
  
        keys = []  
        while len(keys) < len(digits):  
            keys.extend(self.key)  
        while len(keys) > len(digits):  
            del keys[-1]  
        #print([a+b-1 for a,b in zip(digits,keys)])  
        return ''.join([self.abc[a+b-1] for a,b in zip(digits,keys)])  
  
    def decode(self, word):  
        digits = [self.abc.rfind(k)+1 for k in word.upper()]  
  
        keys = []  
        while len(keys) < len(digits):  
            keys.extend(self.key)  
        while len(keys) > len(digits):  
            del keys[-1]  
        return ''.join([self.abc[a-b-1] for a,b in zip(digits,keys)])
```

Figure 4.1: рис.1. Gamma.

2. Проверим работу алгоритма. (рис. 2)

```
Ввод [79]: A = Gamma('ГАЛЛА')  
  
Ввод [80]: A.code('ПРИКАЗ')  
Out[80]: 'УСХЧБЛ'  
  
Ввод [81]: A.decode('УСХЧБЛ')  
Out[81]: 'ПРИКАЗ'  
  
Ввод [82]: B = Gamma('БУЛАТ')  
  
Ввод [83]: B.code('ЯЛЮБЛЮКУШАТЬ')  
Out[83]: 'БАКВЯДЫЛЖЬФЯЭ'  
  
Ввод [84]: B.decode('БАКВЯДЫЛЖЬФЯЭ')  
Out[84]: 'ЯЛЮБЛЮКУШАТЬ'  
  
Ввод [ ]:
```

Figure 4.2: рис.2. Гаммирование в действии.

5 Библиография

1. ТУИС РУДН
2. <https://ru.wikipedia.org/wiki/%D0%93%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%E>

6 Выводы

Во время выполнения лабораторной работы я освоил на практике шифрование гаммированием.