

Отчет по лабораторной работе 7

Дисциплина: Информационная безопасность

Савченков Дмитрий Андреевич, НПИбд-02-18

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы:	6
3	Выводы	7
	Список литературы	8

List of Figures

2.1	Задание №1	6
2.2	Задание №2	6

List of Tables

1 Цель работы

Освоить на практике применение режима однократного гаммирования

2 Выполнение лабораторной работы:

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определил вид шифротекста при известном ключе и известном открытом тексте.(рис. 2.1).

```
In [1]: #Task #1
def cypher(text, code):
    if len(text) != len(code):
        return None
    return ''.join(chr(ord(a) ^ ord(b)) for a,b in zip(text,code))

In [2]: cypher('Выполнил на питоне!', 'Выполнил на плесах!')
Out[2]: '\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x03\x7f\r\r\x00'

In [3]: cypher('\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x03\x7f\r\r\x00', 'Выполнил на плесах!')
Out[3]: 'Выполнил на питоне!'

In [5]: cypher('С Новым Годом, друзья!', 'С Новым Счастлием, друг')
Out[5]: '\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x03\x7f-4E\x08\x03\x0c\x0c\x0c'

In [6]: cypher('\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x03\x7f-4E\x08\x03\x0c\x0c\x0c', 'С Новым Счастлием, друг')
Out[6]: 'С Новым Годом, друзья!'

In [ ]:
```

Figure 2.1: Задание №1

2. Определил ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.(рис. 2.2).

```
In [1]: #Task #2
def cypher(text, code):
    if len(text) != len(code):
        return None
    return ''.join(chr(ord(a) ^ ord(b)) for a,b in zip(text,code))

In [10]: cypher('С Новым Годом,друзья!', '\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00')
Out[10]: 'С Новым Годом,друзья!'

In [ ]:
```

Figure 2.2: Задание №2

3 Выводы

Освоил на практике применение режима однократного гаммирования.

Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов