

Отчёт

по лабораторной работе 8

Кочетов Андрей Владимирович

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	8

List of Figures

3.1	рис.1. Начало	7
3.2	рис.2. Конец	7

List of Tables

1 Цель работы

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

2 Задание

Написание программы по шифрованию.

3 Выполнение лабораторной работы

1. Выбрал язык программирования(Python) и написал начало программы, как в предыдущей лабораторной работе(рис.1).

```
jupyter Untitled Last Checkpoint: 14 минут назад (unsaved changes)
File Edit View Insert Cell Kernel Widgets Help Trusted Python
import string

In [11]: def generate_key(length, symbols = string.ascii_letters + string.digits):
         return ''.join(random.choice(symbols) for i in range(length))

         def gamming(text, key):
             text_conv = [ord(i) for i in text]
             key_conv = [ord(i) for i in key]
             return ''.join(chr(a ^ b) for a, b in zip(text_conv, key_conv))

In [12]: text = 'С Новым Годом, друзья!'
         key = generate_key(len(text))
         text_shift = gamming(text, key)
         print('Изданный шифротекст:', text_shift)

         Вид шифротекста: рЪёХёВёХёАёГёДёЕёЖёЁёЯё

In [13]: gamming(gamming(text, key), key)
Out[13]: 'С Новым Годом, друзья!'

In [14]: key_2 = generate_key(len(text))
         text_2 = gamming(text, key_2)
         print('Зашифрованный текст:', text_2)
```

Figure 3.1: рис.1. Начало

2. Дописал программу и дешифровал текст без использования ключа(рис.2).

```
[13]: gaming(gaming(text, key), key)
[13]: 'С Новым Годом, друзья!'

[14]: key_2 = generate_key(len(text))
      text_2 = gaming(text_shift, key_2)
      print('Расшифрованный текст: ', text_2)
      Расшифрованный текст: й;сВлЗдЫЮю9||тмНёгФ

[16]: P1 = 'НайвашкохвиюТ1204'
      P2 = '8Северныйфильманка'
      key = generate_key(len(P1))
      C1 = gaming(P1, key)
      C2 = gaming(P2, key)
      print('C1:', C1)
      print('C2:', C2)
      C1: оРуР@WetwEgWhE[]{
      C2: yUfTmUBufseGwhYkVnH

[19]: summa = gaming(C1, C2)
      P1_uncyfered = gaming(summa, p2)
      print(P1_uncyfered)
      НайвашкохвиюТ1204
```

Figure 3.2: рис.2. Конец

4 Выводы

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