

Отчет по лабораторной работе №8

**Элементы криптографии. Шифрование (кодирование) различных
исходных текстов одним ключом**

Александр Олегович Воробьев

Содержание

1	Цель работы	3
2	Последовательность выполнения работы	4
3	Выводы	5

1 Цель работы

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

2 Последовательность выполнения работы

1. прописал блок функции для расчетов.

```
In [3]: import string
import random

In [4]: def hexx(text):
        return " ".join(hex(ord(i))[2:] for i in text)

        def gen_key(size):
            return "".join(random.choice(string.ascii_letters + string.digits) for _ in range(size))

        def encrypted(firstText, secondText):
            first_text = [ord(i) for i in firstText]
            second_text = [ord(i) for i in secondText]
            return "".join(chr(a^b) for a, b in zip(first_text, second_text))
```

Figure 2.1: Блок функции для расчетов

2. Прописал блок обработки данных

```
In [9]: T1 = "НаВашисходящийот1204"
        T2 = "ВСеверныйфилиалБанка"

        key = gen_key(len(T1))
        print("Ключ:", key)
        hex_key = hexx(key)
        print("Ключ в шестнадцатеричном виде:", hex_key)

        C1 = encrypted(T1, key)
        C2 = encrypted(T2, key)

        print("Шифрованный текст:", C1)
        print("Шифрованный текст:", C2)

        decrypt = encrypted(C1, C2)

        print("расшифрованный текст:", encrypted(decrypt, T2))
        print("расшифрованный текст:", encrypted(decrypt, T1))

        Ключ: EWdbQDlVno0GhNlhBKqz
        Ключ в шестнадцатеричном виде: 45 57 64 62 51 44 6c 76 4e 6f 4f 47 68 48 6c 68 42 4b 71 7a
        Шифрованный текст: jAVYj53gTtEYeyf5syuN
        Шифрованный текст: iVee6e6eNУ5c6i4vYy
        расшифрованный текст: НаВашисходящийот1204
        расшифрованный текст: ВСеверныйфилиалБанка
```

Figure 2.2: Блок обработки данных

3 Выводы

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