

Отчет по лабораторной работе №8

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

Легиньких Галина Андреевна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Вывод	8

Список иллюстраций

2.1	Ключ	6
2.2	Шифрование и дешифрование	6
2.3	Предложения	6
2.4	Запуск функций	7
2.5	Вывод	7

Список таблиц

1 Цель работы

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

2 Выполнение лабораторной работы

1. Написала функцию для генерации randomного ключа(состоит из случайно последовательности символов). (рис. 2.1)

```
import random

def generate_key(word):
    key = ""
    for _ in range(len(word)):
        key += random.choice("0123456789abcdef") # Шестнадцатеричная система
    return key
```

Рис. 2.1: Ключ

2. Добавила функцию для шифрования и дешифрования. (рис. 2.2)

```
def en_de_crypt(text, key):
    new_text = ""
    for i in range(len(text)):
        new_text += chr(ord(text[i])^ord(key[i%len(key)]))
    return new_text
```

Рис. 2.2: Шифрование и дешифрование

3. Задала два предложения одной длины. (рис. 2.3)

```
text_1 = 'Машина быстро проехала мимо парка'
text_2 = 'Кошка тихо спала на мягком диване'
```

Рис. 2.3: Предложения

4. Использовала один ключ для шифрования и дешифрования обоих предложений. (рис. 2.4)

```

key = generate_key(text_1)
en_text_1 = en_de_crypt(text_1, key)
de_text_1 = en_de_crypt(en_text_1, key)
en_text_2 = en_de_crypt(text_2, key)
de_text_2 = en_de_crypt(en_text_2, key)

print("Ключ -", key)
print("Текст 1", "\nЗашифрованный текст -", en_text_1, "\nДешифрованный текст -", de_text_1)
print("Текст 2", "\nЗашифрованный текст -", en_text_2, "\nДешифрованный текст -", de_text_2)

```

Рис. 2.4: Запуск функций

5. После запуска получилось вот это. (рис. 2.5)

```

Ключ - eb3fb0222bc4ac7bf48601021733be5af
Текст 1
Зашифрованный текст - 0jћoуuÈƒġ0уUCVıCJTjĚđІѢЄ»ўЉЃЙ!!йsvћі
Дешифрованный текст - Машина быстро проехала мимо парка
Текст 2
Зашифрованный текст - wќoќћ»ѰњvќCvŷġќћfљJ—ќđġцћ!!їњїSќġ
Дешифрованный текст - Кошка тихо спала на мягком диване

```

Рис. 2.5: Вывод

3 Вывод

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