

Лабораторная работа №8

**Элементы криптографии. Шифрование различных исходных текстов
одним ключом**

Кувшинова К.О. группа НФИ-02-19

Содержание

1	Цель работы	4
2	Указания к работе	5
3	Задание к лабораторной работе	6
4	Выполнение лабораторной работы	7
5	Вывод	10
6	Библиография	11

List of Figures

2.1	Схема однократного гаммирования одним ключом двух видов открытого текста	5
4.1	Импорт библиотек	7
4.2	Функции формирования ключа, перевода данных в 16 систему и шифрования	8
4.3	Шифрование и дешифрование текстов	9

1 Цель работы

Целью данной лабораторной работы является освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

2 Указания к работе

Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой: (fig. 2.1)

$$\begin{aligned}C_1 &= P_1 \oplus K, \\C_2 &= P_2 \oplus K.\end{aligned}$$

Figure 2.1: Схема однократного гаммирования одним ключом двух видов открытого текста

3 Задание к лабораторной работе

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитав оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочесть оба текста, не зная ключа и не стремясь его определить.

4 Выполнение лабораторной работы

1. Импортируем необходимые для работы библиотеки (fig. 4.1)

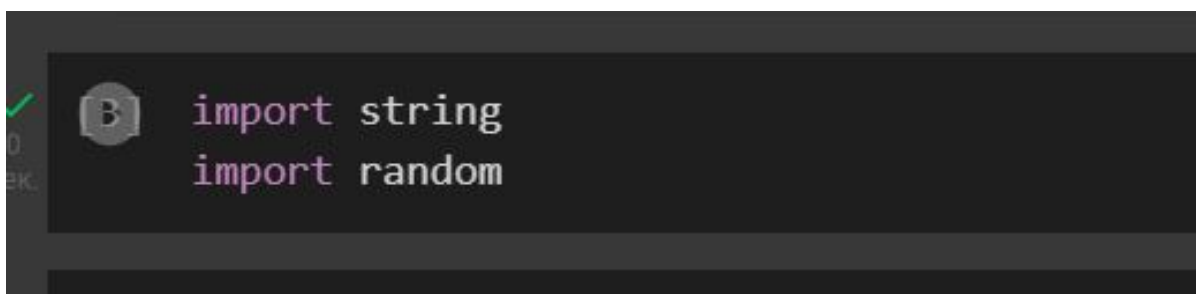


Figure 4.1: Импорт библиотек

2. Напишем функции формирования ключа, перевода данных в 16 систему и шифрования текста. (fig. 4.2)

```

[4] #формирование ключа
def key(size):
    #генерируем ключ
    key1 = ''.join(random.choice(string.ascii_letters+string.digits) for _ in range(size))
    print("Key: ", key1)
    #переводим в 16 СИ
    key2 = coding(key1)
    print("Key in 16: ", key2)
    return key2

#функция перевода в 16 СИ
def coding(smith):
    smith1 = ' '.join(hex(ord(i))[2:] for i in smith)
    return smith1

#шифрование
def crypt(text, key):
    t = [ord(i) for i in text]
    k = [ord(j) for j in key]
    sixt_t=''.join(chr(i^j) for i,j in zip(t,k))
    return sixt_t

```

✓ 0 сек. выполнено в 22:12

Figure 4.2: Функции формирования ключа, перевода данных в 16 систему и шифрования

3. Зашифруем и дешифруем тексты P1 и P2 2 в режиме однократного гаммирования. (fig. 4.3)


```
P1 = "I'm so lonely"
P2 = "Broken angels"

key = key(len(P1))

cp1 = crypt(P1, key)
cp2 = crypt(P2, key)
print("Зашифрованный текст1: ", cp1)
print("Зашифрованный текст2: ", cp2)

decrypt = crypt(cp1, cp2)
finp1 = crypt(decrypt, P2)
finp2 = crypt(decrypt, P1)

print("Расшифрованный текст1: ", finp1)
print("Расшифрованный текст1: ", finp2)

Key: WFR1TNs3Q0fff
Key in 16: 57 46 52 31 54 4e 73 33 51 30 66 66 66
Зашифрованный текст1: |MEO^O]TLL
Зашифрованный текст2: wEO_SN$NTTLF
Расшифрованный текст1: I'm so lonely
Расшифрованный текст1: Broken angels
```

Figure 4.3: Шифрование и дешифрование текстов

5 Вывод

В ходе выполнения лабораторной работы мы освоили на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

6 Библиография

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом [Текст] / Кулябов Д. С., Королькова А. В., Геворкян М. Н. - Москва: - 3 с. [^1]: Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом.