

**Лабораторная работа № 8. Элементы
криптографии. Шифрование
(кодирование) различных исходных
текстов одним ключом**

Ильин Никита Евгеньевич, НФИбд-01-19

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение работы	7
4	Выводы	9
5	Библиография	10

List of Figures

3.1	функции	7
3.2	работа программы	8

List of Tables

1 Цель работы

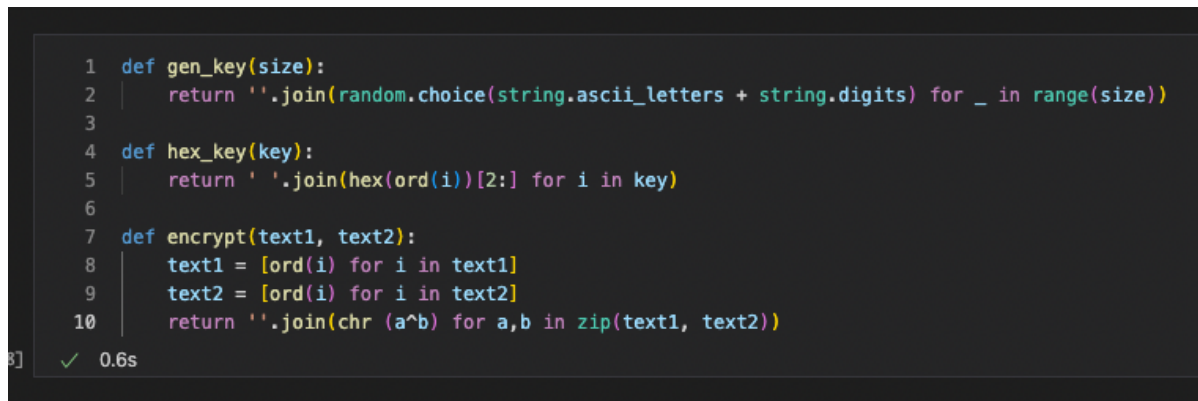
Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом [1].

2 Задание

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочесть оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P_1 и P_2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C_1 и C_2 обоих текстов P_1 и P_2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочесть оба текста, не зная ключа и не стремясь его определить.

3 Выполнение работы

1. Была написана программа, которая соответствует требованиям задачи, и проверяет полученный ключ с изначально сгенерированным.



```
1 def gen_key(size):
2     return ''.join(random.choice(string.ascii_letters + string.digits) for _ in range(size))
3
4 def hex_key(key):
5     return ' '.join(hex(ord(i))[2:] for i in key)
6
7 def encrypt(text1, text2):
8     text1 = [ord(i) for i in text1]
9     text2 = [ord(i) for i in text2]
10    return ''.join(chr (a^b) for a,b in zip(text1, text2))
```

8] ✓ 0.6s

Figure 3.1: функции

```
1 p1 = 'НаВашисходящийот1204'
2 p2 = 'ВСеверныйфилиалБанка'
✓ 0.3s

1 key = gen_key(len(p1))
2 key
✓ 0.2s

'URaMpcKMn0i7mwCp1Sw5'

1 hex_k = hex_key(key)
2 print('Ключ в шестнадцатиричном виде: ')
3 hex_k
✓ 0.4s

Ключ в шестнадцатиричном виде:

'55 52 61 4d 70 63 4b 4d 6e 4f 69 37 6d 77 43 70 31 53 77 35'

1 c1 = encrypt(p1, key)
2 c2 = encrypt(p2, key)
3 
4 print('Зашифрованный текст: ')
5 print(c1)
6 print(c2)
✓ 0.5s

Зашифрованный текст:
шЪёићћJèçЦёсюёваG
чёёwxYŮIiћёKsчowЁёёS

1 decrypt = encrypt(c1, c2)
2 print('Расшифрованный текст: ')
3 print(encrypt(decrypt, p1))
4 print(encrypt(decrypt, p2))
✓ 0.5s

Расшифрованный текст:
ВСеверныйфилиалБанка
НаВашисходящийот1204
```

Figure 3.2: работа программы

4 Выводы

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

5 Библиография

1. Методические материалы курса