

# Лабораторная работа № 8

---

Казакова Виктория Алексеевна

2023, Москва

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

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  $P_1$  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 прочитать оба текста, не зная ключа и не стремясь его определить.

Создала функцию шифрования. Данная функция шифрования получает на вход два текста. Функция `ord` выдает код символа. `Return` перебирает символы. Для пары символов взяли `zip`.

```
def sewing(text1, text2):  
    text1 = [ord(i) for i in text1]  
    text2 = [ord(i) for i in text2]  
    return ''.join(chr(a^b) for a, b in zip(text1, text2))
```

Рис. 1: Функция шифрования

Ввела данные из условия. Зашифровала текст с помощью ключа K, вывела данные

```
P1 = "НаВашисходящийот1204"  
P2 = "ВСеверныйфилиалБанка"  
K = "05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54"  
  
C1 = sewing(P1, K)  
C2 = sewing(P2, K)  
  
print("Зашифрованный текст P1: ", C1)  
print("Зашифрованный текст P2: ", C2)
```

Рис. 2: Шифрование текста

Создаю последовательность, с помощью которой происходит расшифровка текста. Расшифрую при помощи нее текст и вывожу их в дополнительные переменные.

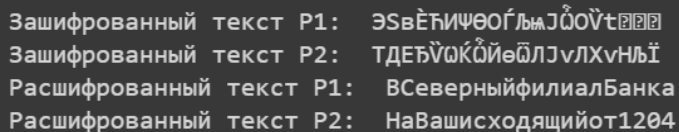
```
X = sewing(C1, C2)

C3 = sewing(X, P1)
C4 = sewing(X, P2)

print("Расшифрованный текст P1: ", C3)
print("Расшифрованный текст P2: ", C4)
```

Рис. 3: Перешифровка текста

Запустим программу и получим результат.



```
Зашифрованный текст P1: ЭSвЁИΨΘΟΓЬжJŮOÛt??  
Зашифрованный текст P2: ТДЕЪÛŲKŲЙёŲLJvLXvNЬİ  
Расшифрованный текст P1: ВСеверныйфилиалБанка  
Расшифрованный текст P2: НаВашисходящийот1204
```

**Рис. 4:** Результат

В ходе работы было освоено на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.