

# Лабораторная работа № 8

---

Тарусов Артём Сергеевич

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, 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.

Создаем функцию шифрования.

```
In [3]: def ecncrypt(t1, t2):  
        t1 = [ord(i) for i in t1]  
        t2 = [ord(i) for i in t2]  
        return ''.join(chr(a^b) for a, b in zip(t1, t2))
```

**Рис. 1:** Функция шифрования

Введем данные из условия.

```
In [4]: 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"
```

**Рис. 2:** Данные из условия

Зашифруем текст с помощью ключа К.

```
C1 = encrypt(P1, K)
C2 = encrypt(P2, K)

print("Зашифрованный текст C1:", C1)
print("Зашифрованный текст C2:", C2)
```

**Рис. 3:** Шифрование текста

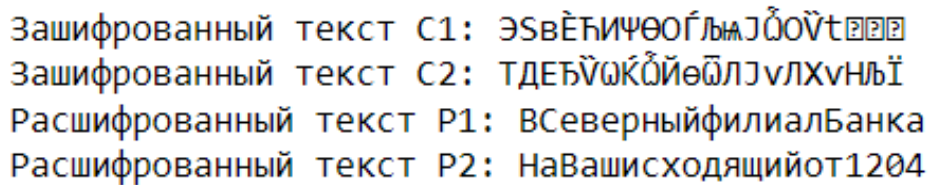
Создадим последовательность, с помощью которой будем расшифровывать текст. Передадим ее в функцию шифрования вместе с зашифрованным текстом.

```
decr = ecncrypt(C1, C2)

print("Расшифрованный текст P1:", ecncrypt(decr, P1))
print("Расшифрованный текст P2:", ecncrypt(decr, P2))
```

**Рис. 4:** Расшифровка текста

Запустим программу и получим результат.



The image shows a screenshot of a program's output. It contains four lines of text, each starting with a label followed by a colon. The first two lines are for encrypted text (C1 and C2), and the next two are for decrypted text (P1 and P2). The text is displayed in a monospaced font with a light blue background.

Зашифрованный текст C1: ЭSвÈҢИΨΘOГльAJŒOÛt???

Зашифрованный текст C2: ТДЕЪÛΩKŒЙёŒЛJvлXvнЬİ

Расшифрованный текст P1: ВСеверныйфилиалБанка

Расшифрованный текст P2: НаВашисходящийот1204

Рис. 5: Результат



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