

# Лабораторная работа № 8

---

Юрченко Артём Алексеевич

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.

Создаем функцию шифрования.

```
: def encrypt(plaintext, key):  
    encrypted_text = ""  
    key_length = len(key)  
    for i in range(len(plaintext)):  
        char = plaintext[i]  
        key_char = key[i % key_length]  
        encrypted_text += chr((ord(char) + ord(key_char)) % 256) # Применение шифра Цезаря  
    return encrypted_text
```

**Рис. 1:** Функция шифрования

Введем данные из условия.

```
plain_text_1 = "навашисходящийот1204"  
plain_text_2 = "ВСеверныйфилиалБанка"  
key = "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.

```
cipher_text_1 = encrypt(plain_text_1, key)
cipher_text_2 = encrypt(plain_text_2, key)
print("Зашифрованный текст (1):", cipher_text_1)
print("Зашифрованный текст (2):", cipher_text_2)
```

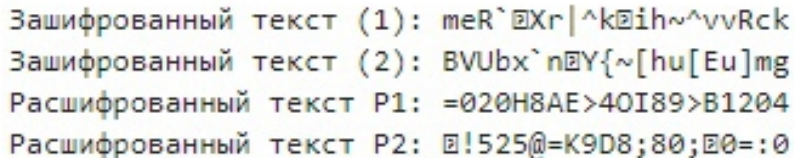
**Рис. 3:** Шифрование текста

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

```
decrypted_1 = decrypt(cipher_text_1, key)
decrypted_2 = decrypt(cipher_text_2, key)
print("Расшифрованный текст P1:", decrypted_1)
print("Расшифрованный текст P2:", decrypted_2)
```

**Рис. 4:** Расшифровка текста

Запустим программу и получим результат.



```
Зашифрованный текст (1): meR`@Xr|^k@ih~^vvRck
Зашифрованный текст (2): BVUbx`n@Y{~[hu[Eu]mg
Расшифрованный текст P1: =020H8AE>4OI89>B1204
Расшифрованный текст P2: @!525@=K9D8;80;@0=:0
```

**Рис. 5:** Результат



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