

## Лабораторная работа 8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

---

Панченко Д. Д.

11 мая 2024

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Панченко Денис Дмитриевич
- Студент 2 курса факультета физико-математических наук.
- Российский университет дружбы народов
- [derenchikde@gmail.com](mailto:derenchikde@gmail.com)

- Цель: Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.
- Задачи:
  - Научиться применять режим однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

## Выполнение лабораторной работы

---

1) Создадим файл с программой.

A terminal window with a dark background. The prompt is [ddpanchenko@derenchik ~]\$ and the command entered is nano shifr1.py.

```
[ddpanchenko@derenchik ~]$ nano shifr1.py
```

Рис. 1: Файл с программой

## 2) Напишем саму программу для шифрования.

```
GNU nano 5.6.1                                shifr1.py                                Modifi
def encrypt(text, key):
    text_bytes = bytearray(text, 'utf-8')
    key_bytes = bytearray.fromhex(key)

    encrypted_text = bytearray(len(text_bytes))
    for i in range(len(text_bytes)):
        encrypted_text[i] = text_bytes[i] ^ key_bytes[i % len(key_bytes)]

    return encrypted_text

def decrypt(encrypted_text, key):
    key_bytes = bytearray.fromhex(key)

    decrypted_text = bytearray(len(encrypted_text))
    for i in range(len(encrypted_text)):
        decrypted_text[i] = encrypted_text[i] ^ key_bytes[i % len(key_bytes)]

    return decrypted_text.decode('utf-8')

def analyze_texts(encrypted_text1, encrypted_text2, known_text1):
    decrypted_known_text1 = bytearray(known_text1, 'utf-8')
    analyzed_text2 = bytearray(len(encrypted_text2))
    min_length = min(len(encrypted_text1), len(encrypted_text2), len(decrypted_known_text1))
    for i in range(min_length):
        analyzed_text2[i] = encrypted_text1[i] ^ encrypted_text2[i] ^ decrypted_known_text1[i]

    return analyzed_text2.decode('utf-8')

P1 = "НаВашисходящийот1204"
P2 = "ВСеверныйфилиалБанка"
K = "050C177F0E4E37D29410092E2257FFC808B27054"

encrypted_text1 = encrypt(P1, K)
encrypted_text2 = encrypt(P2, K)

decrypted_text1 = decrypt(encrypted_text1, K)
decrypted_text2 = decrypt(encrypted_text2, K)

known_text1 = "НаВашисходящийот"
```

3) Выполним эту программу.

```
[ddpanchenko@derenchik ~]$ python shifr1.py  
P1: НаВашисходящийот1204  
P2: ВСеверныйфилиалБанка  
Analyzed P2: ВСеверныйфилиалБ
```

Рис. 3: Выполнение программы



## Вывод

---

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