

# Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

---

Губина О. В.

18 октября 2023

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Губина Ольга Вячеславовна
- студент(-ка) уч. группы НПИбд-01-20
- Российский университет дружбы народов
- 1032201737@pfur.ru
- <https://github.com/ovgubina>

## Вводная часть

---

- Необходимость знания шифрования на практике для обеспечения информационной безопасности.

- Симметричное шифрование, гаммирование.

- Освоить на практике применение режима однократного гаммирования.
- Написать программу осуществляющую шифрование.

- Язык программирования Python



## Процесс выполнения работы

---

## Создание алфавита для осуществления кодирования, гамма и текст для шифрования

```
gamma = "безопаснаяпередачаданных"
text = "сновымгодом"

alphabet = {"а" :0, "б" :1 , "в" :2 , "г" :3 , "д" :4 , "е" :5 , "ё" :6 , "ж" : 7,
            "з" : 8, "и" : 9, "й" : 10, "к" : 11, "л" : 12, "м" : 13, "н" : 14,
            "о" : 15, "п" : 16, "р" : 17, "с" : 18, "т" : 19, "у" : 20, "ф" : 21,
            "х" : 22, "ц" : 23, "ч" : 24, "ш" : 25, "щ" : 26, "ъ" : 27, "ы" : 28,
            "ь" : 29, "э" : 30, "ю" : 31, "я" : 32
            } # это алфавит, где буква - ключ, а номер - значение

# создаем словарь для обратного определения букв по числу
alphabet_2 = {v: k for k, v in dict.items() }
```

```
text_nums = list() # числа букв по алфавиту
gamma_nums = list() # то же самое для гаммы

# в созданный список запишем числа букв из текста
for i in text:
    text_nums.append(alphabet[i])

# print("Числа текста", text_nums)

# в созданный список запишем числа букв из гаммы
for i in gamma:
    gamma_nums.append(alphabet[i])
```

## Шифрование цифрами по принципу сложения по модулю 33 - число знаков алфавита

```
result_nums = list() # результат

ch = 0 # шифруем по принципу остатка от деления числа буквы, на ко-во символов
# в алфавите
for i in text:
    try:
        a = alphabet[i] + gamma_nums[ch]
    except:
        ch=0
        a = alphabet[i] + gamma_nums[ch]
    if a >= 33:
        a = a % 33
    ch+=1
    result_nums.append(a)
```

## Создание кодированного текста через полученные цифры

```
# теперь обратно числа представим в виде букв
text_encrypted = ""

for i in result_nums:
    text_encrypted += alphabet_2[i]

print("Зашифрованный текст:", text_encrypted)
```

## Дешифрование текста

```
#теперь приступим к реализации алгоритма дешифровки
listofdigits = list()
for i in text_encrypted:
    listofdigits.append(alphabet[i])
ch = 0
listofdigits1 = list()
for i in listofdigits:
    a = i - gamma_nums[ch]
    #проблемы тут могут быть
    if a < 0:
        a = 32 + a
    listofdigits1.append(a)
    ch+=1
textdecrypted = ""
for i in listofdigits1:
    textdecrypted+=alphabet_2[i]
print("Расшифрованный текст:", textdecrypted)
```

Зашифрованный текст: ттцркмфьднь

Расшифрованный текст: сновъмгоднм

Зашифрованный текст: ойъ

Расшифрованный текст: нет

## Результаты работы

---



- Написала программу осуществляющую шифрование.

## Вывод

---

Освоила на практике применение режима однократного гаммирования.