

# **Отчёт по лабораторной работе №3**

**Шифрование гаммированием**

Александр Олегович Воробьев

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Выводы</b>	<b>8</b>
	<b>Список литературы</b>	<b>9</b>

# List of Figures

2.1	Код 1	. . . . .	6
2.2	Код 2	. . . . .	6
2.3	Код 3	. . . . .	7

## List of Tables

# **1 Цель работы**

Приобрести практические навыки шифрования гаммированием.

## 2 Выполнение лабораторной работы

### 1. На языке Python реализовал выбор алфавита и его генерацию.

```
[1] import numpy as np

[2] def get_alph(option):
    if option=="eng":
        return list(map(chr, range(ord("a"), ord("z") + 1)))
    elif option=="rus":
        return list(map(chr, range(ord("а"), ord("я") + 1)))
    else:
        print("введите eng или rus")
```

Figure 2.1: Код 1

### 2. Далее реализовал алгоритм шифрования гаммированием.

```
def gamma_encrypt(message: str, gamma: str):
    alph = get_alph("eng")
    if message.lower() not in alph:
        alph = get_alph("rus")
    print(alph)
    m = len(alph)
    def encrypt(letters_pair: tuple):
        idx = (letters_pair[0] + 1) + (letters_pair[1] + 1) % m
        if idx > m:
            idx = idx - m
        return idx - 1

    message_clear = list(filter(lambda s: s.lower() in alph, message))
    gamma_clear = list(filter(lambda s: s.lower() in alph, gamma))
    message_ind = list(map(lambda s: alph.index(s.lower()), message_clear))
    gamma_ind = list(map(lambda s: alph.index(s.lower()), gamma_clear))

    for i in range(len(message_ind) - len(gamma_ind)):
        gamma_ind.append(gamma_ind[i])
    print(f'{message.upper()} -> {message_ind}\n{gamma.upper()} -> {gamma_ind}')
    encrypted_ind = list(map(lambda s: encrypt(s), zip(message_ind, gamma_ind)))
    print(f'encrypted form: {encrypted_ind}\n')
    return ''.join(list(map(lambda s: alph[s], encrypted_ind))).upper()
```

Figure 2.2: Код 2

### 3. Ввел данные для проверки.

```
[4] def test_encryption(message: str, gamma:str):
    print(f'encryption result: {gamma_encrypt(message, gamma)}')
```

message = "приказ"  
gamma = "гамма"  
test\_encryption(message, gamma)

['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ъ', 'ы', 'ь', 'э', 'ю', 'я', ' ']  
ПРИКАЗ -> [15, 16, 8, 10, 0, 7]  
ГАММА -> [3, 0, 12, 12, 0, 3]  
encrypted form: [19, 17, 21, 23, 1, 11]  
encryption result: УСХЧБЛ

Figure 2.3: Код 3

## **3 Выводы**

Приобрел практические навыки реализации шифрования гаммированием.



## Список литературы

1. Кулябов Д.С. Лабораторная работа No 3. Шифрование гаммированием [Электронный ресурс]. – 3 с.