

# **Отчёт по лабораторной работе №7**

**Элементы криптографии. Однократное гаммирование**

Артамонов Тимофей Евгеньевич

# Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	7
4	Выводы	9
	Список литературы	10

## Список иллюстраций

3.1	Код. Часть 1 . . . . .	7
3.2	Получили один из вариантов написания “С новым годом, друзья!”	8

## **Список таблиц**

# **1 Цель работы**

Освоить на практике применение режима однократного гаммирования.

## 2 Теоретическое введение

Гаммирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в “наложении” последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле. Например, в поле Галуа суммирование принимает вид операции “исключающее ИЛИ (XOR)”. [1]

### 3 Выполнение лабораторной работы

Напишем функции на python и зададим переменные. (рис. [3.1])

```
import random
import string
✓ 0.0s

def xor_text(text, key):
    result = ""
    for i in range(len(text)):
        result += chr(ord(text[i]) ^ ord(key[i]))
    return result
✓ 0.0s

def key_gen(text):
    key = ""
    for i in range(len(text)):
        key += random.choice(string.ascii_letters + string.digits)
    return key
✓ 0.0s

def part_key(fragment, encrypted):
    first = xor_text(fragment, encrypted[:len(fragment)])
    return first + key_gen(encrypted[len(fragment):])
✓ 0.0s

text = "Новый формат, друзья!"
fragment = "Новый"
```

Рис. 3.1: Код. Часть 1

Применим написанные функции для создания ключа, шифрования текста и дешифрования. (рис. [3.2])

```
encrypted = xor_text(text, key_gen(text))
encrypted
[6] ✓ 0.0s
... 'КєψκнVГмщіJV{\x18йñйè0To'

try_ = part_key(fragment, encrypted)
xor_text(encrypted, try_)
[7] ✓ 0.0s
... 'С новымг.ІЯпᐁр>)цOVЪћē:'
```

Рис. 3.2: Получили один из вариантов написания “С новым годом, друзья!”



## **4 Выводы**

Освоили на практике применение режима однократного гаммирования.

# Список литературы

1. Гаммирование [Электронный ресурс]. Wikimedia Foundation, Inc., 2024. URL: [https://en.wikipedia.org/wiki/XOR\\_cipher](https://en.wikipedia.org/wiki/XOR_cipher).