# Лабораторная работа №7

## Основы информационной безопасности

Волгин Иван Алексеевич

11 мая 2024

Российский университет дружбы народов, Москва, Россия

# Цель работы

Освоить на практике применение режима однократного гаммирования.

# Задание

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно: 1. Определить вид шифротекста при известном ключе и известном открытом тексте. 2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

# Выполнение лабораторной работы

# 1. Для начала создаю функцию, которая будет генерировать случайный ключ (рис. 1).

```python
def hex_key_gen(text):
    key = ''
    for i in range(len(text)):
        key += random.choice(string.ascii_letters + string.digits)
    return key
```

**Рис. 1:** генерация случайного ключа

## 2. Затем пишу функцию для шифрования и дешифрования текста (рис. 2).

```
def crypt(text,key):
    new_text = ''
    for i in range(len(text)):
        new_text += chr(ord(text[i]) ^ ord(key[i % len(key)]))
    return new_text
```

**Рис. 2:** шифрование текста

# 3. После пишу функцию, которая будет находить различные возможные ключи для определенного фрагмента, с помощью которых

шифротекст может быть преобразован в фрагмент (рис. 3).

```
def find_key(text, fragment):
    possible_keys = []
    for i in range(len(text) - len(fragment) + 1):
        possible_key = ""
        for j in range(len(fragment)):
            possible_key += chr(ord(text[i+j]) ^ ord(fragment[j]))
        possible_keys.append(possible_key)
    return possible_keys
```

**Рис. 3:** поиск ключей

# 4. После этого проверяю работу всех функций, все работает корректно (рис. 4).

```
print('Текст:', t, '\nКлюч', key, '\nШифротекст', en_t)
print('Возможные ключи:', keys)
print('Расшифрованный фрагмент:', crypt(en_t, key[0]))
```

```
Текст: С Новым Годом, друзья!
Ключ ahSE8Oth6w5nLXLZ7jq7ZT
Шифротекст pHюоЂєшHXщЁёЧtlЋVЩЦцоЁu
Возможные ключи: ['ahSE8Ot', 'ѡЋf46\x03V', 'oЋ\x17:zf\x19', 'Zb\x19vÒnu', '•ΦЏЎ\x17\x02¤', '%Ѭs\x1b{Jl', 'ih8ѡ3\x1bL', 'ѡST?b;
ш', '\x04ѧ\x1cnBnѧ', 'hCMNЦчR', ' Ψmьў%K', 'qёмЋ\\<\x15', 'QTψPEbz', 'sLsI\x1b\rG', 'эмj\x17t0)', 'OЇ4x1^ц']
ЦЖшЧKVШованный фрагмент: С)ЯКжЩ)ФШбБШ
```

**Рис. 4:** проверка работы кода

# Выводы

Я освоила на практике применение режима однократного гаммирования.

Спасибо за внимание!