

Отчёт

по лабораторной работе 7

Агеева Анастасия Борисовна

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	9

List of Figures

3.1	рис.1. Программа.	7
3.2	рис.2. Определение ключа.	7

List of Tables

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 Задание

Лабораторная работа подразумевает подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

3 Выполнение лабораторной работы

1. Разработаем приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. (рис.1).

```
In [66]: from itertools import zip_longest, cycle

def xor_crypt_string(data: str, key: str):
    xored = ''
    for (x, y) in zip_longest(data, cycle(key)):
        if not x:
            break
        xored += chr(ord(x) ^ ord(y))
    return xored

a = xor_crypt_string('С новым годом, друзья!', '1231212121212121213')
print(a)
print(xor_crypt_string(a, '1231212121212121213'))

АҮӲЄӧӱЄӲӱӳSӨSӇ
С новым годом, друзья!

In [67]: xor_crypt_string('А•ӲӱЄӧӱ•ЄӲӲӱӳ••SӨSӇ••', '1231212121212121213')

Out[67]: 'С новым годом, друзья!'
```

Figure 3.1: рис.1. Программа.

2. Подберём ключ, чтобы получить сообщение «С Новым Годом Вас!». После ключа текст становится неизменным. (рис.2).

```
In [77]: xor_crypt_string('С новым годом, друзья!', '\x00/\x00\x00\x00\x00\x00\x00\x00\x00/\x00:\x00,\x00;\x00'\x00/\x00\x00\x00')
Out[77]: 'С новым годом, друзья'
```

Figure 3.2: рис.2. Определение ключа.

3. Контрольные вопросы

- 1) Поясните смысл однократного гаммирования. Каждый символ попарно с символом ключа складываются по модулю.
- 2) Перечислите недостатки однократного гаммирования. Ключ нельзя переиспользовать. Размер ключа должен быть такой же, как и размер текста.

- 3) Перечислите преимущества одноразового гаммирования. Основные преимущества одноразового гаммирования – это симметричность и криптостойкость.
- 4) Почему длина открытого текста должна совпадать с длиной ключа? Потому что каждый символ открытого текста должен складываться символом ключа попарно.
- 5) Какая операция используется в режиме одноразового гаммирования, назовите её особенности? В режиме одноразового гаммирования используется сложение по модулю 2. Её особенность состоит в том, что при сложении чисел с другим получается исходное. Например, $0+0=0$, $0+1=1$, $1+0=1$, $1+1=0$.
- 6) Как по открытому тексту и ключу получить шифротекст? Нужно сложить попарно символы текста с ключом по модулю 2.
- 7) Как по открытому тексту и шифротексту получить ключ? Нужно сложить попарно символы открытого текста с символами шифротекста по модулю 2.
- 8) В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра? Необходимые и достаточные условия абсолютной стойкости шифра: а) полная случайность ключа; б) равенство длин ключа и открытого текста; в) использование ключа однократно.

4 Выводы

Я приобрела практические навыки применения режима однократного гаммирования.