### Отчет по лабораторной работе №8

Информационная безопасность

Евдокимова Юлия Констинтиновна НПИбд-01-18

# Содержание

| 1 | Цель работы                    | 4  |
|---|--------------------------------|----|
| 2 | Выполнение лабораторной работы | 5  |
| 3 | Контрольные вопросы            | 8  |
| 4 | Выводы                         | 10 |

# **List of Figures**

| 2 1 | Вывод |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   | 7 |
|-----|-------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4.1 | рывод | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • |

## 1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

#### 2 Выполнение лабораторной работы

1. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты Р1 и Р2. Приложение должно определить вид шифротекстов С1 и С2 обоих текстов при известном ключе.

Для разработки используем наработки из лабораторной работы 7. Старый код:

```
def gamm(t_text, t_key):
    res = ''
    for i, j in zip(t_text, t_key):
        temp=chr(ord(i) ^ ord(j))
        res+=temp
    return res

P1 = 'C Новым годом, друзья!'
P2 = ''
Key = 'лабораторная работа н7'

P2 = gamm(P1, Key)
print(P2)

p_result = gamm(P2, P1)
print(p_result)

Новый код:
```

```
def gamm(t_text, t_key):
    res = ''
    for i, j in zip(t_text, t_key):
        if i == '-':
            temp='-'
        else:
            temp = chr(ord(i) ^ ord(j))
        res += temp
    return res
Р1 = 'С Новым годом, друзья!'
Р2 = 'лабораторная работа н7'
Key = 'qwertyuiopasdfqhjklzxc'
C1 = gamm(P1, Key)
C2 = gamm(P2, Key)
print(C1, C2, '\n')
t P1 = '- -овы- го-о-, -руз-я!'
t_C = gamm(C1, C2)
t_P2 = gamm(t_P1, t_C)
print(t_P1)
print(t_P2)
  1. В функцию gamm добавлена возможность игнорировать отмеченные мину-
    сом символы
  2. Переменные Р - два текста.
    Кеу - ключ
    С - шифротексты.
```

Злоумышленник знает часть текста - t P1, шифротексты C1/C2

- t C результат гаммирования C1 и C2
- t P2 неизвестный текст 2, который в дальнейшем будет выяснен.
  - 3. Задаем переменные
  - 4. Гаммируем Р1 и Р2 по ключу, получаем С1 и С2
  - 5. Злоумышленник знает С1 и С2, поэтому гаммирует их.
  - 6. Затем злоумышленник гаммирует t\_P1 по получившемуся значению, получает t P2.
  - 7. Теперь по имеющимся текстам можно подставить свои предположительные значения и гаммировать их по тому же значению, чтобы пошагово получать всё больше символов из Р1 и Р2. В данном случае будет достигнуто либо полное открытие всех символов обоих текстов, либо сужение круга возможных решений.
  - 8. Вывод программы:

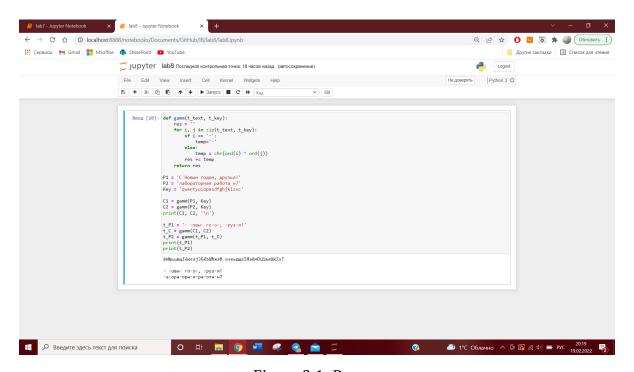


Figure 2.1: Вывод

#### 3 Контрольные вопросы

1. Как, зная один из текстов ( $P_1$  или  $P_2$ ), определить другой, не зная при этом ключа?

По формуле  $C_1 \oplus C_2 \oplus P_1 = P_1 \oplus P_2 \oplus P_1 = P_2$ 

- 2. Что будет при повторном использовании ключа при шифровании текста? Текст расшифруется.
- 3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов? по формулам режима однократного гаммирования:

$$C_1 = P_1 \oplus K_1$$

$$C_2 = P_2 \oplus K_2$$

- 4. Перечислите недостатки шифрования одним ключом двух открытых текстов.
  - ключ, попав не в те руки, даст возможность злоумышленнику расшифровать оба текста;
  - можно расшифровать с помощью открытого текста другие известные шифротексты;

- можно узнать часть текста, используя заранее известный шаблон и формат другого текста.
- 5. Перечислите преимущества шифрования одним ключом двух открытых текстов.
- скорость шифрования выше;
- простой алгоритм шифрования;
- шифротекст сильно меняется, если изменяется ключ или открытый текст.

#### 4 Выводы

На основе проделанной работы освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.