

# Отчет по лабораторной работе №8

---

Коломиец Мария Владимировна НПИбд-01-18<sup>1</sup>

Информационная Безопасность–2021, 10 декабря, 2021, Москва,  
Россия

<sup>1</sup>Российский Университет Дружбы Народов

# Цели и задачи работы

---

## Цель лабораторной работы

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

## Задание к лабораторной работе

Два текста кодируются одним ключом. Требуется, не зная ключа и не стремясь его определить, прочитав оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты  $P_1$  и  $P_2$  в режиме однократного гаммирования. Приложение должно определить вид шифротекстов  $C_1$  и  $C_2$  обоих текстов  $P_1$  и  $P_2$  при известном ключе. Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочесть оба текста, не зная ключа и не стремясь его определить.

# **Процесс выполнения лабораторной работы**

---

1. Создаем алфавит из русских букв и цифр. Задаем входные данные из условия лабораторной работы. (рис. 1).

```
a = ord("a")
alphabeth = [chr(i) for i in range(a, a + 32)]
a = ord("0")
for i in range(a, a+10):
    alphabeth.append(chr(i))

a = ord("А")
for i in range(1040, 1072):
    alphabeth.append(chr(i))
print(alphabeth)
P1 = "НаВашисходящийот1204"
P2 = "ВСеверныйфилиалБанка"

key = "05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54"
```

**Рис. 1:** Создание алфавита

## 2. Функция “vzlom”, которая получив два открытых сообщения и объединив их получает гамму. (рис. 2).

```
def vzlom(P1, P2):
    code = []
    for i in range(26):
        code.append(alphabeth[(alphabeth.index(P1[i]) + alphabeth.index(P2[i])) % len(alphabeth)])
    print(code)
    print(code[5], " ", code[19])
    p3 = "".join(code)
    print(p3)

vzlom(P1, P2)

['a', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z']
['a', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z']
['d', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z']
['d', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z']
['d', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z']
d e f g h i j k l m n o p q r s t u v w x y z
1 2 3 4
```

Рис. 2: Функция “vzlom”

3. Функция “shifr”, которая получает исходные сообщения (рис. 3).

[illegible]

**Рис. 3: Функция “shifr”**



## 4. Алгоритм расшифровки, вывод программы. (рис. 4).

```
listofdigits1 = list()
for i in listofdigits:
    try:
        a = i - listofdigitsofgamma[ch]
    except:
        ch=0
        a = 1 - listofdigitsofgamma[ch]
    if a < 1:
        a = 75 + a
    listofdigits1.append(a)
    ch += 1
textdecrypted = ""
for i in listofdigits1:
    textdecrypted += dict2[i]
print("Расшифрованный текст:", textdecrypted)

shifr(P1)

Введите гамму(на русском языке)на3звезда74pdy1E44
Числа текста [47, 1, 35, 1, 26, 18, 19, 23, 16, 5, 32, 27, 18, 11, 16, 28, 66, 67, 75, 69]
Числа гаммы [27, 51, 41, 3, 31, 26, 32, 48, 25, 26, 72, 69, 18, 11, 27, 53, 66, 38, 33, 69]
1
29
21
57
38
33
63
Числа зашифрованного текста [74, 52, 1, 4, 57, 36, 51, 63, 41, 31, 29, 21, 28, 22, 43, 73, 57, 38, 33, 63]
Зашифрованный текст: 8TayЧC33nuyR0VnA3
Расшифрованный текст: НовиковаВиктор1284
```

Рис. 4: Результат”

## **Выводы по проделанной работе**

---

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

# **Контрольные вопросы**

---

## Контрольные вопросы

1. Как, зная один из текстов ( $P_1$  или  $P_2$ ), определить другой, не зная при этом ключа?
2. Что будет при повторном использовании ключа при шифровании текста?
3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?
4. Перечислите недостатки шифрования одним ключом двух открытых текстов.
5. Перечислите преимущества шифрования одним ключом двух открытых текстов.