# Лабораторная работа № 8

**Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом**

Казакова Виктория Алексеевна

# Содержание

# Список иллюстраций

# 1 Цель работы

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

# 2 Задание

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

# 3 Ход работы

1. Создала функцию шифрования (рис. 3.1). Данная функция шифрования получает на вход два текста. Функция ord выдает код символа. Return перебирает символы. Для пары символов взяли zip.

```
def sewing(text1, text2):
  text1 = [ord(i) for i in text1]
  text2 = [ord(i) for i in text2]
  return ''.join(chr(a^b) for a, b in zip(text1, text2))
```

Рис. 3.1: Функция шифрования

2. Ввела данные из условия. Зашифровала текст с помощью ключа K, вывела данные. (рис. 3.2).

```
P1 = "НаВашисходящийот1204"
P2 = "ВСеверныйфилиалБанка"
K = "05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 OB B2 70 54"

C1 = sewing(P1, K)
C2 = sewing(P2, K)

print("Зашифрованный текст P1: ", C1)
print("Зашифрованный текст P2: ", C2)
```

Рис. 3.2: Шифрование текста

3. Создала последовательность, с помощью которой происходит расшифровка текста. Расшифроваю при помощи нее текст и вывожу их в дополнительные переменные.(рис.@fig:003).

```
X = sewing(C1, C2)

C3 = sewing(X, P1)
C4 = sewing(X, P2)

print("Расшифрованный текст P1: ", C3)
print("Расшифрованный текст P2: ", C4)
```

Рис. 3.3: Перешифровка текста

4. Запустила программу и получила результат. (рис. 3.4).

```
Зашифрованный текст P1:  ЭSвÈЂИΨΘOЃЉЊJЊOЎt□□□
Зашифрованный текст P2:  ТДЕЂЎЩЌЊЙөЋЛJvЛXvНЉЇ
Расшифрованный текст P1:  ВСеверныйфилиалБанка
Расшифрованный текст P2:  НаВашисходящийот1204
```

Рис. 3.4: Результат

# 4 Вывод

В ходе работы я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# 5 Список литературы


1. [Методический материал 1] [https://esystem.rudn.ru/pluginfile.php/2090284/mod_resource/c
lab_crypto-gamma.pdf]
2. [Методический материал 2] [https://esystem.rudn.ru/pluginfile.php/2090286/mod_resource/c
lab_crypto-key.pdf]
3. [Google Colab] [https://colab.research.google.com/?hl=ru]