

## Лабораторная работа 3

Попов Дмитрий Павлович, НФИмд-01-23

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра математического моделирования и искусственного интеллекта

ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

дисциплина: Математические основы защиты информации и информационной безопасности

Преподаватель: Кулябов Дмитрий Сергеевич

Студент: Попов Дмитрий Павлович

Группа: НФИмд-01-23

МОСКВА

2023 г.

# **Прагматика выполнения лабораторной работы**

# Прагматика выполнения лабораторной работы

► Требуется реализовать:

1. Шифрование гаммированием конечной гаммой

## Цель работы

# Цель работы

Приобретение практических навыков в шифровании гаммированием.

## **Выполнение лабораторной работы**

1. Реализовал программу для шифрования гаммированием конечной гаммой ( $1/2$ )



# 1. Реализовал программу для шифрования гаммированием конечной гаммой (1/2)

```
1 print("-----")
2 print(" Шифрование гаммированием")
3 print("-----")
4
5
6 def crypt(mess, gamma, alphabet):
7     # делаем гамму по длине больше, чем сообщение для шифрования
8     while len(gamma) < len(mess):
9         gamma += gamma
10
11     # создаем списки из номеров букв из алфавита в сообщении и гамме
12     mess_numb, gamma_numb, cypher_numb = [], [], []
13     for symbol in mess:
14         mess_numb.append(alphabet.index(symbol) + 1)
15     for symbol in gamma:
16         gamma_numb.append(alphabet.index(symbol) + 1)
17     # шифруем сообщение по рекуррентной формуле
18     cypher_mess = ''
19     for i in range(0, len(mess_numb)):
20         c = mess_numb[i] + gamma_numb[i] % len(alphabet)
21         cypher_numb.append(c)
22         cypher_mess += str(alphabet[c - 1])
```

Figure 1: gamma1

1. Реализовал программу для шифрования гаммированием конечной гаммой (2/2)

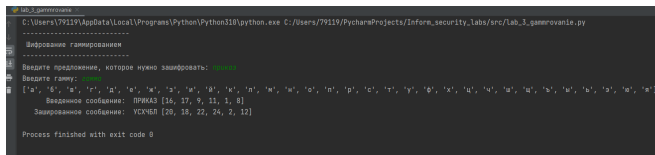
# 1. Реализовал программу для шифрования гаммированием конечной гаммой (2/2)

```
22     print(alphabet)
23     print("    Введенное сообщение: ", mess.upper(), mess_numb)
24     print("    Зашированное сообщение: ", cypher_mess.upper(), cypher_numb)
25
26
27     alphabet = ['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о',
28                'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ь', 'ы', 'ь', 'а', 'ю', 'я']
29     mess = str(input("Введите предложение, которое нужно зашифровать: ")).lower().replace(' ', '')
30     # mess = 'приказ'.replace(' ', '')
31     gamma = str(input("Введите гамму: ")).lower()
32     # gamma = 'гамма'
33
34     crypt(mess=mess, gamma=gamma, alphabet=alphabet)
```

Figure 2: gamma2

## 2. Вывод работы программы

## 2. Вывод работы программы



```
lab_3_gamma_out.exe
C:\Users\79119\AppData\Local\Programs\Python\Python310\python.exe C:/Users/79119/PycharmProjects/Inform_security_labs/src/lab_3_gamma_out.py
-----
Шифрование гаммированием
-----
Введите предложение, которое нужно зашифровать: ПРИКАЗ
Введите гамму: 16179118
['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ъ', 'ы', 'я', ' ', 'a']
Введенное сообщение: ПРИКАЗ [16, 17, 9, 11, 1, 8]
Зашифрованное сообщение: VСХЧБЛ [20, 18, 22, 24, 2, 12]

Process finished with exit code 0
```

Figure 3: gamma\_out

## Вывод

## Вывод

В результате выполнения работы я освоил на практике применение шифрования с гаммированием конечной гаммой.

