МИНОБРНАУКИ РОССИИ

Изображение выглядит как текст

Автоматически созданное описаниеФедеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра информатики и систем управления

Отчет

По лабораторной работе №2

«Шифрование методом гаммирования»

По дисциплине

«Защита информации»

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Капранов С.Н.

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Игнаков К. М.

(подпись) (фамилия, и.,о.)

19-ВМ

(шифр группы)

Работа защищена «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород 2022

**Задание №2.1.**

Реализовать алгоритм шифрования данных «Шифрование методом гаммирования» по модулю N.

**Шифрование методом гаммирования по модулю N.**

Метод гаммирования заключается в «наложении» ключа на открытый текст. А метод по модулю N является операцией «XOR» или исключающим ИЛИ. Это операция является обратной, поэтому шифрование и расшифровывание проводится одинакого.

**Алгоритм.**

1. Сначала вводим сообщение, которое будем кодировать/декодировать.

2. Вводим ключ, с помощью которого будем кодировать/декодировать.

3. Далее проводим кодирование с использованием исключающего ИЛИ между сообщением и ключом.

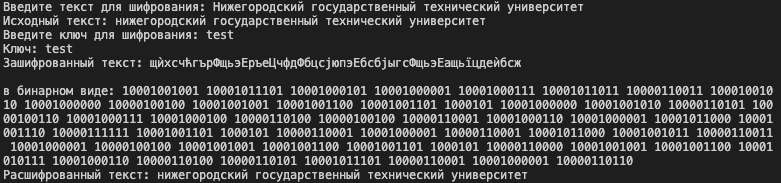
4. Выводим зашифрованное сообщение.

5. Проводим декодирование с использованием исключающего ИЛИ между зашифрованным сообщением и ключом.

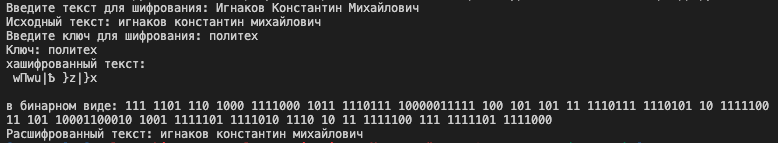
6. Выводим расшифрованное сообщение.

**Примеры шифрования/расшифровывания.**

1. Нижегородский государственный технический университет:



1. Игнаков Константин Михайлович:



**Текст программы.**

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

if \_\_name\_\_ == '\_\_main\_\_':

print('Исходный текст:', text := input("Введите текст для шифрования: ").strip().lower().replace('ё', 'е'))

print('Ключ:', key := str(input("Введите ключ для шифрования: ")))

encode\_text = xor\_crypt\_string(text, key)

print('Зашифрованный текст:', encode\_text, '\n\nв бинарном виде:', ' '.join(format(ord(x), 'b') for x in encode\_text))

decode\_text = xor\_crypt\_string(encode\_text, key)

print('Расшифрованный текст:', decode\_text)