МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ

УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ

(национальный исследовательский университет)»

Институт №3 «Системы управления, информатика и электроэнергетика»

Кафедра 311 «Прикладные программные средства и математические методы»

**Лабораторная работа №5**

по дисциплине:

«Информационная безопасность»

на тему:

**«**Гаммирование»

Работу выполнил:

студент гр. М3О-318Бк-19

Артиков Темур Улугбекович

Научный руководитель:

ассистент, Кос О.И.

Дата выдачи задания: 18.09.2021 .

Дата сдачи: 04.12.2021 .

.

Москва 2021 г.

Оглавление:

Глава 1: Введение…………………………………………………………………

Глава 2: Алгоритм для реализации………………………………………………

Глава 3: Код программы………………………………………………………….

Глава 4: Демонстрация работы………………………………………………......

Выводы………...…………………………………………………………………..

Список литературы………………………………………………………………..

**Глава 1: Введение**

**Цель работы:** программирование шифра Гаммирование (шифрование, дешифрование)

Данная лабораторная работа была выполнена с помощью языка программирования Python в среде программирования

**Глава 2: Алгоритм для реализации**

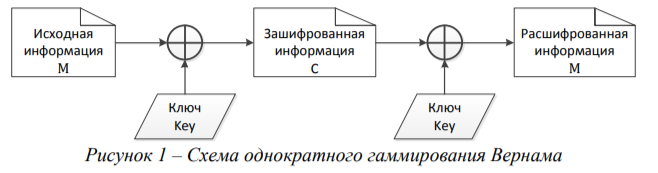
Простейшей и в то же время наиболее надёжной из всех схем шифрования является так называемая схема однократного использования (см. рисунок 1), изобретение, которое чаще всего связывают с именем Г.С. Вернама. Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. С точки зрения теории криптоанализа, метод шифрования случайной однократной равновероятной гаммой той же длины, что и открытый текст, является не вскрываемым (далее для краткости будем употреблять термин "однократное гаммирование", держа в уме всё сказанное выше). Кроме того, даже раскрыв часть сообщения, дешифровщик не сможет хоть сколько-нибудь поправить положение – информация о вскрытом участке гаммы не даёт информации об остальных её частях.

Допустим, в тайной деловой переписке используется метод однократного наложения гаммы на открытый текст. "Наложение" гаммы – не что иное, как выполнение операции сложения по модулю 2 (xor) её элементов с элементами открытого текста. Эта операция в языке программирования Python обозначается знаком ^, а в математике – знаком .

**Стандартные операции над битами:**

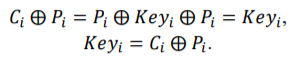
****

Гаммирование является симметричным алгоритмом. Поскольку двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, шифрование и дешифрование выполняется одной и той же программой. Режим шифрования однократного гаммирования реализуется следующим образом:



Задача нахождения шифротекста при известном ключе и открытом тексте состоит в применении следующего правила к каждому символу открытого текста:

 (1)

где – i-й символ получившегося зашифрованного текста,  – i-й символ открытого текста,  – i-й символ ключа, где Размерности открытого текста и ключа должны совпадать, тогда полученный шифротекст будет такой же длины. Задача нахождения ключа по известному шифротексту и открытому тексту может быть решена, исходя из (1). Для этого нужно обе части равенства сложить  с по модулю 2:

(2)

(3)

Таким образом получаются формулы для решения обеих поставленных задач. Т.к. открытый текст представлен в символьном виде, а ключ – в своём шестнадцатеричном представлении, то в соответствие с таблицей ASCII-кодов можно представить ключ в символьном виде. Тогда уже будут возможны операции (1), (3), необходимые для решения поставленных задач.

**Глава 3: Код программы**

mode = input('Viberite mode: [E]ncrypt ||| [D]ecrypt: ')

if mode == 'E':

message = list(input("Vashe slovo: "))

key = input("Vash kluch: ")

for symbol in range(len(message)):

try: message[symbol] = chr(ord(message[symbol]) ^ int(key))

except ValueError: message[symbol] = chr(ord(message[symbol]) ^ ord(key))

print("Vash zashifrovanniy text:","".join(message))

with open("crypt.txt","w") as file:

file.write("".join(message))

print(message)

elif mode == 'D':

message = list(input("Vash shifr: "))

key = input("Vash kluch: ")

for symbol in range(len(message)):

try: message[symbol] = chr(ord(message[symbol]) ^ int(key))

except ValueError: message[symbol] = chr(ord(message[symbol]) ^ ord(key))

print("Vashe isxodnoe slovo:","".join(message))

**Глава 4: Демонстрация работы**

1. Выбираем функцию шифрования - 1. Далее следует ввод текста и выбор гаммы «key». На выходе работы программы получаем шифрованный текст «rijvs uyvjn».

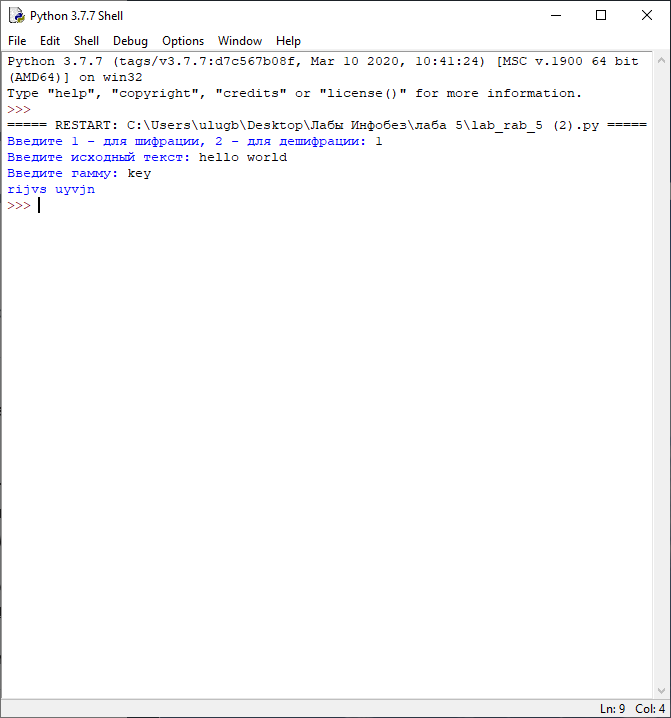


Рисунок 1 – Функции шифрования.

1. Работа функции дешифрования. Выбираем функцию дешифрования – 2. Затем следует ввод шифрованного текста «rijvs uyvjn» и ввод гаммы «key»

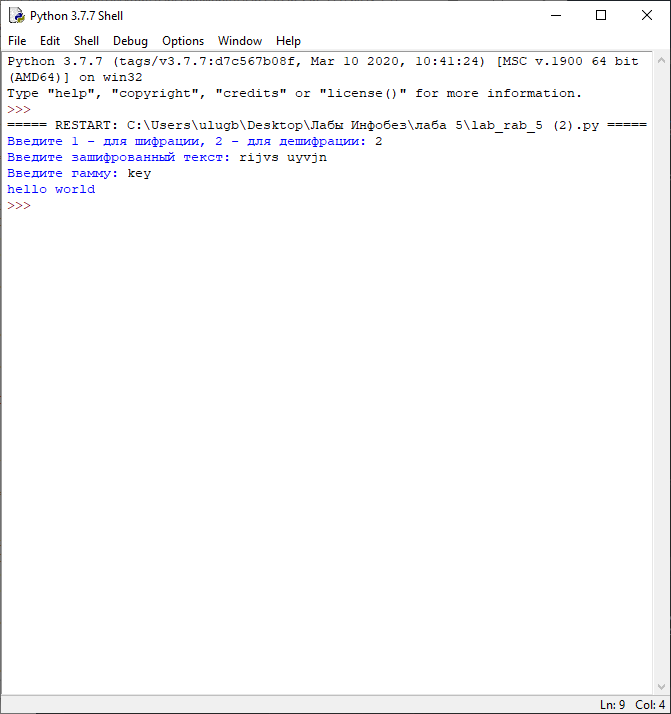


Рисунок 2 – Функция дешифрования.

**Результаты тестирования программы:**

1. Ввод: «hello world». Гамма: «key». Вывод: «rijvs uyvjn»
2. Ввод: «rijvs uyvjn». Гамма: «key». Вывод: «hello world»

**Выводы**

В данной лабораторной работе я изучил метод шифрования Гаммирование.

Список литературы:

1. Гаммирование. <https://ru.wikipedia.org/wiki/%D0%93%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5>