МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

**Факультет информационных технологий и робототехники (ФИТР**)

Кафедра программного обеспечения информационных систем и технологий

**Отчёт по лабораторной работе №2**

по дисциплине: “Основы защиты информации”

на тему:**“Классические методы шифрования”**

Вариант 5

Выполнил: ст. гр. 10702119      Кислицин Данила Андреевич

Проверила:                                                                       Белова Светлана Владимировна

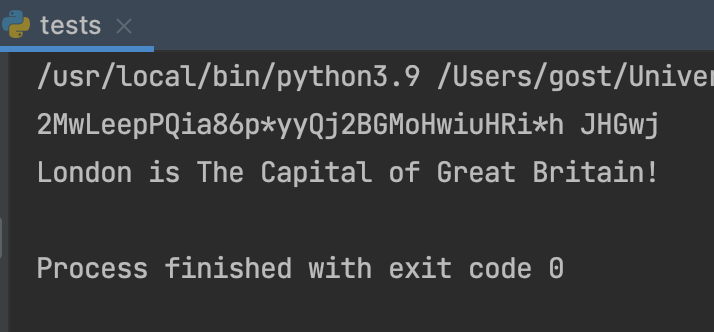
Минск 2021

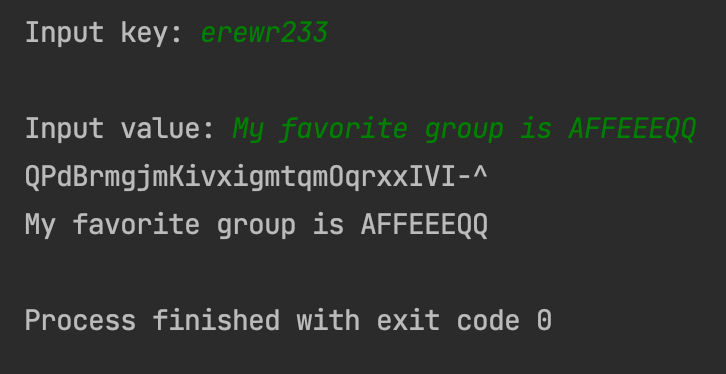
**Лабораторная работа №2**

**“Классические методы шифрования”**

**Цель:** познакомиться с основными криптографическими терминами и моделью традиционного шифрования. Изучить типы криптосистем. Изучить особенности классических методов шифрования на примере конкретных алгоритмов.

**Задание:** Шифр, использующий сложение с ключевым словом (Латинский)

**Результаты работы:**

*Рис.1. – Результаты выполнения шифрования и расшифрования.*

*Рис.2. – Результат выполнения контрольного задания.*

**Контрольные вопросы:**

1. Сформулируйте правило Керкхоффа.

*Сложность шифра должна определяться только секретностью ключа, а не секретностью алгоритма.*

2. Что такое шифрование, расшифрование, криптосистема, алфавит, открытый текст, пространство ключей?

1. *Шифрование – обратимое преобразование информации с помощью алгоритма шифрования и ключа.*
2. *Расшифрование – процедура, обратная шифрованию, преобразование шифртекста в открытый текст с помощью алгоритма и ключа лицами, владеющими ключом на законном основании.*
3. *Криптосистема – алгоритм шифрования + соответствующий ему алгоритм расшифрования.*
4. *Алфавит – символы, используемые алгоритмом шифрования.*
5. *Открытый текст – исходное сообщение.*
6. *Пространство ключей – множество всех возможных ключей, доступных в алгоритме.*

3. Какие криптосистемы называют симметричными. Нарисуйте модель симметричной криптосистемы, предложенную К. Шенноном, и запишите формулы шифрования и расшифрования?

*Симметричные шифры (симметричные криптосистемы) - это шифры, в которых для шифрования и расшифрования используется один и тот же ключ. Их называют еще традиционными криптосистемами, криптосистемами с одним ключом или криптосистемами с секретным ключом.*

*C = Ek(P)*

*P = Dk(C),*

*Где C – шифротекст, P – открытый текст, E – алгоритм шифрования, D – алгоритм расшифрования, K – ключ.*

4. По каким признакам классифицируются криптосистемы?

1. *Число применяемых ключей (симметричные, асимметричные)*
2. *Тип операций по преобразованию открытого текста в шифротекст. (подстановочные, перестановочные, композиционные)*
3. *Метод обработки открытого текста(блочные, поточные)*

5.Какие криптосистемы называются блочными, какие – поточными?

*При создании блочных шифров важнее – стойкость к взлому, в ущерб всему остальному*

*При создании поточных шифров важнее – быстродействие.*

*В случае блочного криптоалгоритма – ожидает поступления порции данных (блока), в случае поточного криптоалгоритма преобразование происходит в реальном (или близком к нему) масштабе времени. Блочный – жестко заданный размер обрабатываемого блока. Поточный – если поступает бит, обрабатывается бит, если слово – то слово.*

*Блочный – каждый блок данных шифруется независимо от других блоковна одном и том же ключе по единому алгоритму. Поточный – каждая порция (элемент) входной последовательности обрабатывается на своем ключе, т.е. поток данных и поток ключей.*

*Блочный – результат шифрования блока не зависит от его позиции в исходном тексте Поточный – результат шифрования порции данных зависит от позиции в исходном тексте.*

6. Чем отличается расшифрование и дешифрование?

*Расшифрование (decryption) – процедура, обратная шифрованию, преобразование шифртекста в открытый текст с помощью алгоритма и ключа лицами, владеющими ключом на законном основании.*

*Дешифрование (deciphering) (взлом, вскрытие шифра) - восстановление исходного текста без знания ключа*

7. Поясните понятия криптография, криптология, криптоанализ,

1. *Криптография – наука о методах преобразования информации с целью её защиты от несанкционированных пользователей.*
2. *Криптология – наука , изучающая шифры и их стойкость.*
3. *Стеганография – сокрытие факта существования сообщения.*
4. *Криптоанализ – наука, изучающая методы взлома шифров.*

8. Какие системы шифрования называют классическими?

Используют ли их на практике? Что общего у классических шифров с современными симметричными криптосистемами?

*Классические – алгоритмы, используемые в докомпьютерную эпоху. В настоящее время они не применяются на практике, так как легко взламываются с помощью современных вычислительных средств. Однако классические шифры представляют исторический и учебный интерес, поскольку основаны на тех же принципах, что и современные шифры. Все они относятся к более широкой группе симметричных шифров. Примерами классических шифров являются шифры Цезаря, Трисемуса, Плейфейера, Уитстона, Виженера, Вернама, «Магический квадрат» и другие*

9. Что такое криптостойкость? В каком случае схема шифрования называется абсолютно стойкой? Приведите пример абсолютно стойкого шифра.

*Криптостойкость – сложность алгоритма раскрытия шифра.*

*Абсолютно стойкой называется схема шифрования, при которой шифротекст не содержит информацию, достаточную для однозначного воссстановления открытого текста.*

*Лента однократного использования(Шифр Вернама + Длина ключа = длина сообщения, ключ – истинно случайная последовательность, ключ используется только один раз)*

10. Какие криптосистемы называют защищенными по вычислениям?

*• Стоимость взлома шифра превышает стоимость расшифрованной информации*

*• Время, которое требуется для того, чтобы взломать шифр, превышает время, в течение которого информация актуальна.*

*Схема шифрования называется защищенной по вычислениям, если она соответствует обоим критериям*

**Вывод:** в данной лабораторной работе познакомились с основными криптографическими терминами и моделью традиционного шифрования. Изучили типы криптосистем. Изучили особенности классических методов шифрования на примере конкретных алгоритмов.

**ЛИСТИНГ ИСХОДНЫХ КОДОВ**

**Decryption.py**

class KeysSum:

def \_\_init\_\_(self):

self.\_alphabet = **"abcdefghijklmnopqrstuvwxyz"** \

**"ABCDEFGHIJKLMNOPQRSTUVWXYZ"** \

**"~`!@#$%^&\*()-\_=+"** \

**"0123456789"** \

**" "**

self.\_alpha\_len = len(self.\_alphabet)

def encrypt(self, key, value):

value\_len = len(value)

while len(key) < value\_len:

key += key

result = **""**

for i in range(value\_len):

x = self.\_alphabet.find(value[i])

k = self.\_alphabet.find(key[i])

y = (x + k) % self.\_alpha\_len

result += self.\_alphabet[y]

return result

def decrypt(self, key, value):

value\_len = len(value)

while len(key) < value\_len:

key += key

result = **""**

for i in range(value\_len):

y = self.\_alphabet.find(value[i])

k = self.\_alphabet.find(key[i])

x = (y - k) % self.\_alpha\_len

result += self.\_alphabet[x]

return result

tests.py

from decryptor import KeysSum

coder = KeysSum()

\_key = input(**"Input key: "**)

\_value = input(**"**\n**Input value: "**)

encoded = coder.encrypt(\_key, \_value)

print(encoded)

decoded = coder.decrypt(\_key, encoded)

print(decoded)