МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное автономное образовательное учреждение высшего образования “Национальный исследовательский университет ИТМО”

ФАКУЛЬТЕТ ПРОГРАММНОЙ ИНЖЕНЕРИИ И КОМПЬЮТЕРНОЙ ТЕХНИКИ

ЛАБОРАТОРНАЯ РАБОТА №1

“ Основы шифрования данных”

из раздела

“Криптографические системы с секретным ключом”

по дисциплине

“Информационная безопасность”

Вариант 1

Выполнил:

Иванов Матвей Сергеевич

группа P34111

Преподаватель:

Маркина Татьяна Анатольевна

г. Санкт-Петербург, 2024

Цель работы:

Изучение основных принципов шифрования информации, знакомство с широко известными алгоритмами шифрования, приобретение навыков их программной реализации.

Листинг программы:

```
import os
from string import printable

rus =
"АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯабвгдеёжзийклмнопрстуфхцчшщъ
ыьэюя«»"
alph = rus + printable

k = int(input("Input K: "))
key_word = input("Input keyword: ")

if len(set(key_word)) != len(key_word):
     print("Keyword should be with unique letters")
     exit(1)

other_let = "".join([char for char in alph if char not in
key_word])
cipher_alph = other_let[-k:] + key_word + other_let[:-k]

assert len(alph) == len(cipher_alph)

filename = input("Input filename: ")

if not os.path.exists(filename):
     print("File not exists")
     exit(1)


with open(filename, "r") as f:
     text = f.read()
```

```
# Encoding

cipher = ""

for char in text:
     if char not in alph:
          print(f"Char not in alphabet! Char: {char}")
          continue

     ind = alph.index(char)
     cipher += cipher_alph[ind]

print("\n\nENCODED:\n")
print(cipher)

# Decode

decoded_text = ""

for char in cipher:
     if char not in cipher_alph:
          print(f"Char not in alphabet! Char: {char}")
          continue

     ind = cipher_alph.index(char)
     decoded_text += alph[ind]

print("\n\nDECODED:\n")
print(decoded_text)
```

Результат работы: