

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 Р34111**

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 =
"АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯабвгдеёжзийклмнопрстуфхцчщъ
ььэюя«»"
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:

```
(base) Joulin@MacBook-Air-39 Downloads % python fb_lab.py
Input K: 3
Input keyword: прикол
Input filename: test_fb_text.txt

ENCODED:

{жзЧЩЕ|вЧевЕБ|адббхх<|ОмЕ|му|ад|дЕОбхх|ЕШбЧЧмц|Щ|ЩЕ|б|ефбзббхх|}фмЕШу|жзЧЩЕ|мЧевЕБ|адббхх<|
|ы|ЯнбШшн|ЯЩЕб|ЩШ|ШнбнцЕЯмц|ад|жЕБШмцмц|}вЕБбЧ|вЕЕфхх|внЗЯ|а|дбЙмЕ|бЕЯмЧевхх<|ЯгхЧГа|дш|ъмЕ|бЧ|Щббц|ъмЕ|Шнвв}

{Ч|мбхбзц<|
|му|фмЕ|мбхбзц|ббгЧбхх<|ЕШазЧбхх|аг|Юб+|Шнбц|ЯббгЧмц|}жЕадЧбхх|му|ъмЕ<|
сЧевЧяв*мЕ|АЩЧЕЕЩфЧ|
ЧгзххвЕ|фб|му|аг|мбзбОбхх|ддгггевбз|Шнбнцб|}мбОб|}аг|ЯнбШшн|зЧжЕгЧбЧмц|дб<|ОбзбЯ|ббЯм*мЕ|гвк|рЧ|Ш|ббЯм*мЕ|гбм|дЧм|нбмбм|ЕЯг|бмнц|бм|вЕбнЕвб|}Ч|жЕБЧнб|фмЕ|а|Ея|ЯгЪЯ|Е
м|жЕЯмЧ|аЯфЧгем.|Ч|ЯбЯмзЧ<|Ен|}жаббгЧб*мЧ|}фмЕ|дЕОбм|Шмц|а|ЯбЯмзЕб|фбзбЯ|ббЯмц|гбм|Чга|Щ|ъм|ббЯмц|гбх<|рЕбЧбЧг|Яс-Яс-Яс|д-фгг|Ее|ЯШш|а|жЕбзЧгЕяЦг|ъмдд|ЩЕкзЕЯЧдв|}бЧОб|Я|аЧад*мЕ|еЧЯгЧОббЕабд*|
жз
Ефбд|}Щб|ъм|ЩЕжЕЯн|Шга|еб|ЕЕШб|}еб|ЩЕЯЧкЕаб|}Ч|ЯмЧзуб|}еЧЩЕгбЦхб|}бЧЩЕахЕаб+|рЧЩЕ|мб|аЧв|Ееа|Ечфгг|ббЕ|мбзЯЧмц|а|аЙмбзЯЧга|бдн|Ябзуб*|рЧЩЕмЧбЧЩЕ|аЧв|ЯЧЕбЯгЧЩ|Щ|Ебд|Шр|ъмЧ|мбхбзхххх|мЕЯвЧ
|еЧЧЧмЧЧ|еЧЕвбн|гЧмц|а|Щ|жЕЯг|мЕбб|Шзбв|ЯбЯв|ЯбЯв|Ч|а|ЯЕу|вЕмззбЦгЧЧд|}жзЕв|сЕдн|мбЧЕЕЕб|}бнЕбб|а|сЧЕчЧмбфЯнбб|ЩЕжЕЯЧ|}вЕмзб|ЯЧднфг|ббЕ|Ябзуб|а|Яд|}ЕЕмзЧдд|мббн|зЧЧзххЕаб*|Ябмзц|Ю
|жзЯдЕ|дЧмбзз|Шзбн|аЧв|ззЕдд|Щ|ЕббЕ|мбЗзгг+|ЦЕЕ|}фмЕ|мбхбзц|сЧмЕ|Шгг|Еб|мЕЯвбЦЧмц|}Еб|ЯмзЧмц|жЧЯаЦЕЕ|}Емдд|зЧЯнОббЕабдд|Е|мдд|}фмЕ|ЩЕжЕЯн|ЕбзЧзбххд|}Ч|ЕбжзбдЕЕЕ|фмЕ*Еалнбц|ЯббгЧмц|}а|Яббф
Чв|Юб|}а|жЕЯвЕзбб*|
Е|фмЕ|Шу|мЕ|Еа|ЯмЧгЕ|еЧмЕ|збххмц|}ТЕмц|еЧ|фмЕ*Еалнбц|}аг+

DECODED:

не бывать? А что же ты делаешь, чтоб этому не бывать? Запретишь? А право какое имеешь? Что ты им можешь обещать в свое очередь, чтобы право такое иметь? Все судьбу свою, всю будущность им посвятить, ко
гда конишь курс и место достанешь? Слышали мы это, да ведь это буки, а теперь? Ведь тут надо теперь же что-нибудь сделать, понимаешь ты это? А ты что теперь делаешь? Обираешь их же. Ведь деньги-то им по
д сторублевый пенсион да под господ Свидригайловых под заклад достаются! От Свидригайловых-то, от Афанасия-то Ивановича Вахрушина чем ты их убережешь, миллионер будущий, Зевес, их судьбою располагающий?
Через десять-то лет? Да в десять-то лет мать успеет ослепнуть от космиков, а пожалуй что и от слез; от поста исчахнет; а сестра? Ну, придумаю-ка, что может быть с сестрой через десять лет али в эти десять
лет? Догадася?»
Так мучил он себя и поддразнивал этими вопросами, даже с каким-то наслаждением. Впрочем, все эти вопросы были не новые, не внезапные, а старые, наболевшие, давшие. Давно уже как они начали его терзать
и истерзали ему сердце. Давным-давно как зародилась в нем вся эта теперешняя тоска, нарастала, накоплялась и в последнее время созрела и концентрировалась, приняв форму ужасного, дикого и фантастическог
о вопроса, который замучил его сердце и ум, неотразимо требуя разрешения. Теперь же письмо матери вдруг как громом в него ударило. Ясно, что теперь надо было не тосковать, не страдать пассивно, одними ра
суждениями о том, что вопросы неразрешимы, а непременно что-нибудь сделать, и сейчас же, и поскорее. Во что бы то ни стало надо решиться, хоть на что-нибудь, или...
```