МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное автономное
образовательное учреждение высшего образования
«Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики»

ФАКУЛЬТЕТ ПРОГРАММНОЙ ИНЖЕНЕРИИ И КОМПЬЮТЕРНОЙ ТЕХНИКИ

ЛАБОРАТОРНАЯ РАБОТА № 1

по дисциплине

‘Информационная безопасность’

‘Основы шифрования данных’

Вариант №9

Выполнил:
Студент группы P34111
Павлов Александр
Сергеевич
Преподаватель:
Маркина Т.А.

Санкт-Петербург, 2024

Цель работы

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

Вариант: реализовать шифрование и дешифрацию файла по методу Виженера с составным ключом. Набор ключей вводится

Программные и аппаратные средства

Процессор: Intel Core i5-11400F 2.6GHz 12 ядер

Видеокарта: NVIDIA GeForce RTX 2060

Объем оперативной памяти: 32 GB

Язык программирования: Python

Листинг разработанной программы с комментариями

```
# Метод Виженера


# for ru.txt keys is ПЕРВЫЙ БУКВА

# for en.txt keys is SOME KEYS IS HERE


ALPHABET_RU = 'АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЫЬЭЮЯ '

ALPHABET_EN = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ '


# Функция для определения языка файла

def detect_language(text):

    if ALPHABET_RU.find(text[0]) != -1:

        return "ru"

    return "en"


# Функция для шифрирования текста

def encrypt(data, keys, alphabet, num):

    answer = ''
```

```
    for i in range(len(data)):
        number = (alphabet.find(data[i]) + sumKeys(keys, i, alphabet)) % num
        answer += alphabet[number]
    return answer

# Функция для дешифрации текста
def decrypt(data, keys, alphabet, num):
    answer = ''

    for i in range(len(data)):
        number = (alphabet.find(data[i]) - sumKeys(keys, i, alphabet))
        if number < 0:
            number += num
        number %= num
        answer += alphabet[number]
    return answer

# Функция для суммирования ключей
def sumKeys(keys, index, alphabet):
    result = 0
    for key in keys:
        result += alphabet.find(key[index % len(key)])

    return result



fileName = str(input("Введите название файла: "))

f = open(fileName, "r", encoding="utf-8")
data = f.read().replace("\n", "")

keys = list(map(str, input("Введите ключи через пробел: ").split(" ")))
```

```
language = detect_language(data)


alphabet = ALPHABET_RU if language == "ru" else ALPHABET_EN

num = 32 if language == "ru" else 27


mode = str(input("Режим шифрования или дешифрования? (encr, decr): "))


if mode == "encr":

   print(encrypt(data, keys, alphabet, num))

else:

   print(decrypt(data, keys, alphabet, num))
```

Результаты работы программы

```
PS C:\only_labs_java\infobez\lab1.1> python -u "c:\only_labs_java\infobez\lab1.1\main.py"
Введите название файла: ru.txt
Введите ключи через пробел: ПЕРВЫЙ БУКВА
Режим шифрования или дешифрования? (encr, decr): encr
МКИГЛЭТЮЭВЫКЛСАЮ БФУРЮХАЮКРЫ ЧПК ОЛЭВ
PS C:\only_labs_java\infobez\lab1.1> python -u "c:\only_labs_java\infobez\lab1.1\main.py"
Введите название файла: ru_decode.txt
Введите ключи через пробел: ПЕРВЫЙ БУКВА
Режим шифрования или дешифрования? (encr, decr): decr
ЭТО СТРОКА ОТКРЫТОГО ИСХОДНОГО ТЕКСТА
PS C:\only_labs_java\infobez\lab1.1> python -u "c:\only_labs_java\infobez\lab1.1\main.py"
Введите название файла: en.txt
Введите ключи через пробел: SOME KEYS IS HERE
Режим шифрования или дешифрования? (encr, decr): encr
IUPIPVZQU NBYEOQIRDJ
PS C:\only_labs_java\infobez\lab1.1> python -u "c:\only_labs_java\infobez\lab1.1\main.py"
Введите название файла: en_decode.txt
Введите ключи через пробел: SOME KEYS IS HERE
Режим шифрования или дешифрования? (encr, decr): decr
THIS IS ENGLISH TEXT
```

Выводы по работе

В результате выполнения лабораторной работы были получены навыки реализации алгоритма Виженера с составным ключом на языке программирования Python.