Университет ИТМО
Факультет ПИиКТ
Информационная безопасность

# Лабораторная работа №1
# «Основы шифрования данных»

Вербовой Александр
Группа P3400
Вариант 4

Санкт-Петербург
2021

### Цель работы

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

### Задание (вариант 4)

Реализовать в программе шифрование и дешифрацию файла с использованием квадрата Полибия, обеспечив его случайное заполнение.

### Описание:

Для работы алгоритма использовался русский алфавит

```
import random
```

```
# создание листа русских букв
a = ord("А")
r_letters = list(''.join([chr(i) for i in range(a, a+32)]))

# делает последовательность случайной
r_letters = random.sample(r_letters, k=len(r_letters))

# добавляет в лист недостающие элементы
while len(r_letters) < 6*6:
    r_letters.append("")
```

```
#квадрат с символами для наглядности
square = []

#создает двумерный массив для хранения таблицы символом
for i in range(6):
    square.append([])
    for j in range(6):
        square[i].append(r_letters[i*6+j])

square
```

```
[['П', 'Ю', 'Л', 'М', 'Щ', 'Ь'],
 ['Н', 'О', 'Т', 'Б', 'Я', 'Ш'],
 ['Р', 'Г', 'С', 'Ф', 'Й', 'Е'],
 ['Ч', 'Ц', 'Д', 'Х', 'В', 'Э'],
 ['И', 'Ъ', 'Ж', 'З', 'А', 'Ы'],
 ['К', 'У', '', '', '', '']]
```

```python
# алгоритм шифрование, использует глобальные переменные
# list r_letters
# array[row][col] square

def encode(s):
    # пропускает на вход только буквы
    s = s.upper()
    s = ''.join(filter(str.isalpha, s))
    message = ""

    for char in s:
        #подходящие строки и стобцы таблицы
        row = r_letters.index(char) // 6 + 1
        col = r_letters.index(char) % 6 + 1

        # избегает несуществующие символы
        if row == 5 and col > 2:
            row = 6

        # смена строк
        if row == 6:
            row = 1
        else:
            row += 1
#         code += str(row) + str(col) + " "
        # Зашифрованое сообщение
        message += square[row-1][col-1]

    return message
```

```python
string_to_encode = "ИТМОФЛЭКС" #строка до шифрования

encoded = encode(string_to_encode) # зашифрованная строка
encoded
```

'КСБГХТЫПД'

```python
# алгоритм дешифрование, использует глобальные переменные
# list r_letters
# array[row][col] square

def decode(s):
    s = s.upper()
    s = ''.join(filter(str.isalpha, s))
    print(s)
    message = ""

    for char in s:
        #строки и стобцы таблицы
        row = r_letters.index(char) // 6 + 1
        col = r_letters.index(char) % 6 + 1

        # избегает несуществующие символы
        if row == 1 and col > 2:
            row = 6

        # смена строк
        if row == 1:
            row = 6
        else:
            row -= 1
#         code += str(row) + str(col) + " "
        # новое сообщение
        message += square[row-1][col-1]
    return message
```

```python
decoded = decode(encoded)
decoded
```

```
КСБГХТЫПД
'ИТМОФЛЭКС'
```

### Вывод

В ходе выполнения лабораторной работы был изучен метод шифрование и дешифрования файла с использованием метода квадрата Полибия. Была реализована программа для шифрования и дешифрования текста с использованием данного метода.