Лабораторная работа 1

Юдин Герман Станиславович, НФИмд-02-23

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1

дисциплина: Математические основы защиты информации и информационной безопасности

Преподователь: Кулябов Дмитрий Сергеевич
Студент: Юдин Герман Станиславович
Группа: НФИмд-02-23

МОСКВА

2023 г.

Прагматика выполнения лабораторной работы

Прагматика выполнения лабораторной работы

Требуется реализовать:

1. Шифр Цезаря с произвольным ключом K.
2. Шифр Атбаш.

Цель работы

Цель работы

Освоить на практике шифры простой замены.

Выполнение лабораторной работы

1. Для реализации шифра Цезаря был написан следующий код:

1. Для реализации шифра Цезаря был написан следующий код:

```
base = ['а', 'б', 'в', 'г', 'д', 'е', 'ё', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф',
        'х', 'ц', 'ч', 'ш', 'щ', 'ъ', 'ы', 'ь', 'э', 'ю', 'я', ' ']

k = int(input("Введите число, на которое хотите сдвинуть шифр: "))

k = k % len(base)

pswd = input("Введите кодовое слово: ").lower()
unique_characters = []

for character in pswd:
    if character not in unique_characters:
        unique_characters.append(character)

for character in base:
    if character not in unique_characters:
        unique_characters.append(character)

begin = unique_characters[len(unique_characters)-k:]
end = unique_characters[:len(unique_characters)-k]

cypher = begin + end
```

Figure 1: Шифр Цезаря (подготовка алфавита)

2. Шифрование фразы:

2. Шифрование фразы:

```
print(base)
print(cypher)

while True:
    string = input("Введите строку, которую хотите зашифровать: ").lower()
    if string == "q":
        break

    result = ""
    for character in string:
        result += cypher[base.index(character)]

    print(result)
```

Figure 2: Шифрование

3. Запуск программы

3. Запуск программы

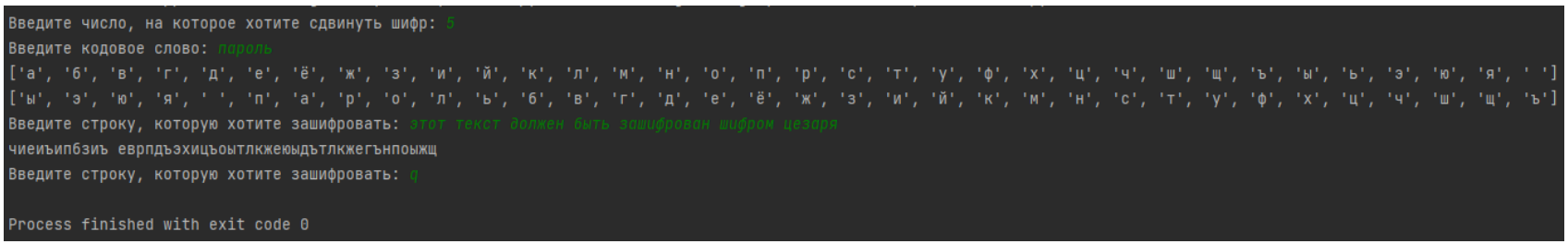

Figure 3: Результат работы

4. Для реализации шифра Атбаш был написан следующий код:

4. Для реализации шифра Атбаш был написан следующий код:

```
base = ['а', 'б', 'в', 'г', 'д', 'е', 'ё', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф',
        'х', 'ц', 'ч', 'ш', 'щ', 'ъ', 'ы', 'ь', 'э', 'ю', 'я', ' ']

cypher = base.copy()
cypher.reverse()

print(base)
print(cypher)

while True:
    string = input("Введите строку, которую хотите зашифровать: ").lower()
    if string == "q":
        break

    result = ""
    for character in string:
        result += cypher[base.index(character)]

    print(result)
```

Figure 4: Код Атбаш

5. Запуск программы

5. Запуск программы

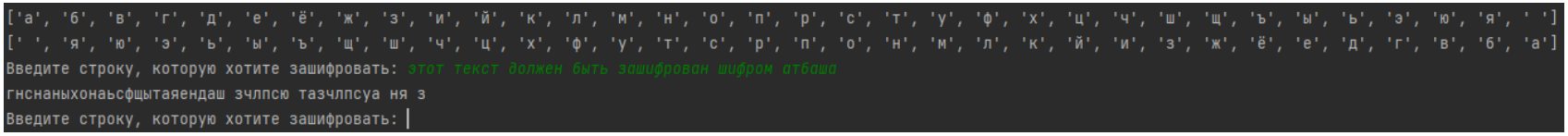

Figure 5: Результат работы

Выводы

Выводы

В результате выполнения работы я освоил на практике применение шифров простой замены.