Отчёт по лабораторной работе №1

Шифр простой замены

Бакундукизе Эжид Принц НФИмд-01-21

Содержание

List of Figures

1 Цель работы

Изучение алгоритмов шифрования Цезаря и Атбаш

2 Теоретические сведения

2.1 Шифр Цезаря

Шифр Цезаря — один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации — шифр простой замены [1]. Например, в шифре со сдвигом 3 А была бы заменена на Г, Б станет Д, и так далее.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и все ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет практически никакого применения на практике.

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики [2]:

```
y = (x + k) mod n
x = (y - k + n) mod n
```

где *x — символ открытого текста,* y — символ шифрованного текста *n — мощность алфавита* k — ключ.

2.2 Шифр Атбаш

Шифр Атбаша является шифром сдвига на всю длину алфавита. Правило шифрования состоит в замене i-й буквы алфавита буквой с номером n − i + 1, где n — число букв в алфавите. Также, как и Шифрование Цезаря является методом простой замены [3].

3 Выполнение работы

3.1 Реализация шифра Цезаря на языке Python

Блок шифрования

```
# функция шифрования по алгоритму цезаря
def tsesar():
    # Объявляем алфавит
    letters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'
    # Задаем шаг в шифровке - на сколько шагов сделать ход по алфавиту.
    step = 5
    # Ввод строки для шифрования
    text = input("Шифрование Цезаря: ")
    #Переменная для результата
    result = ''
    # Шифрование
    for i in text:
        ind = letters.find(i)    # Вычисляем места символов в списке
        newind = ind + step    # Сдвигаем символы на указанный в переменной step
        if i in letters:
            result += letters[newind]  # Задаем значения в итог
        else:
            result += i
    print(result)
```

Блок дешифровки

```
# Дешифрование: вместо добавления шага, вычитаем его и получаем исходное сообщени
def tsesar_deshifr():
    letters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'
    smeshenie = 5
    text = input("Дешифрока Цезаря: ")
    result = ''

    for i in text:
        ind = letters.find(i)
        newind = ind - smeshenie
        if i in letters:
            result += letters[newind]
        else:
            result += i
    print(result)
```

3.2 Реализация шифра Атбаш на языке Python

Блок шифрования

```
# шифр атбаша заключается тупо в том, что меняются буквы
# из обычного алфавита на буквы из алфавита-наоборот
#вместо A идет Z и тп
def atbash():
    # задаем алфавит
    letters = [chr(x) for x in range(65, 91)]
    # алфавит-наоборот
    letters_r = [x for x in letters]
```

```
    letters_r.reverse()

    text = input("Атбаш - шифрование")
    result = ""
    # тут для перебираются буквы из исходного текста
    for i in text:
        # перебираются индексы и значения из letters
        for j,l in enumerate(letters):
            if i == l: # если буквы i и l равны, то
                result += letters_r[j]
        # ставим в результат букву из реверсированного списка с индексом j
    print(result)
```

Блок дешифровки

```
# Дешефровка: меняем местами списки алфавита
def atbash_desh():
    letters = [chr(x) for x in range(65, 91)]
    letters_r = [x for x in letters]
    letters_r.reverse()

    text = input("Атбаш - дешивровка: ")
    result = ""
    for i in text:
        for j, l in enumerate(letters_r):
            if i == l:
                result += letters[j]
    print(result)
```

3.3 Работа алгоритмов

```
if __name__ == "__main__":
    main()
```

```
Шифрование Цезаря: RUDN
WZIS
Дешифрока Цезаря: WZIS
RUDN
Атбаш - шифрование: RUDN
IFWM
Атбаш - дешивровка: IFWM
RUDN
```

Figure 3.1: Работа алгоритмов

4 Выводы

В ходе выполнения данной лабораторной работы мы познакомились с алгортмами шифрования простой замены.

Рассмотрели данный вид алгоритмов на примере шифрования Цезаря и Атбаш. Выполнили программную реализацию этих двух алгоритмов.

Список литературы

1. [Роберт Черчхаус, “Коды и шифры. Юлий Цезарь”]
2. [Гай Светоний Транквилл. Жизнь двенадцати цезарей]
3. [Атбаш (https://www.livelib.ru/book/1001019648-atbash)]