Отчёт по лабораторной работе №1

Шифры простой замены

Волкова Дарья Александровна НПМмд-02-21

Содержание

Цель работы

Изучение шифров простой замены: шифр Цезаря и шифр Атбаш, а также их программная реализация.

Теоретические сведения

Шифр простой замены — один из древнейших. Прежде всего, выбирается нормативный алфавиту т.е. набор символов, которые будут использоваться для составления сообщений. В качестве нормативного алфавита может применяться, например, русский алфавит, исключая буквы «ъ» и «ё». Затем выбирается алфавит шифрования {шифр-алфавит)у который может состоять из произвольных символов (цифр, букв, графических знаков), в том числе и из букв нормативного алфавита. Между нормативным алфавитом и алфавитом шифрования устанавливается взаимно-однозначное соответствие. Такое соответствие обычно задается таблицей и определяет секретный ключ шифра простой замены.

Шифрование заключается в замене каждого символа открытого текста на соответствующие символы шифр-алфавита. В шифре простой замены каждый символ исходного текста заменяется символами шифр-алфавита одинаково на всем протяжении текста.

Шифр Цезаря

Шифр Цезаря, также известный, как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом 3 А была бы заменена на Г, Б станет Д, и так далее.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера. 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:

```
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.

Шифр Атбаш

«Атба́ш» – один из самых древних методов шифрования. Шифрование заключается в замене каждой буквы исходного текста на «симметричную» ей букву алфавита, то есть первая алфавита заменялась на последнюю и наоборот, вторая буква – на предпоследнюю и наоборот и т.д.

Исходный алфавит	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
Алфавит замены:	Я	Ю	Э	Ь	Ы	Щ	Ш	Ч	Ц	Х	Ф	У	Т	С	Р	П	О	Н	М	Л	К	Й	И	З	Ж	Е	Д	Г	В	Б	А

Шифр «атбаш» был, скорее всего, изобретен ессеями, иудейской сектой повстанцев. Они разработали множество различных кодов и шифров, которые использовались для сокрытия важных имен и названий, чтобы потом избежать преследования.

Выполнение работы

Реализация алгоритмов на языке Python

```
# 1. Шифр Цезаря

alphabet = 'абвгдежзийклмнопрстуфхцчшщыьэюя '

message = input('Введите строку: ').lower()
key = int(input('Введите ключ: '))

encrypted = ''

for letter in message:
    if letter in alphabet:
        t = alphabet.find(letter)
        new_key = (t + key) % len(alphabet)
        encrypted += alphabet[new_key]
    else:
        encrypted += letter

print('Криптограмма:', encrypted)

# 2. Шифр Атбаш

alphabet = 'абвгдежзийклмнопрстуфхцчшщыьэюя '

alphabet_revers= alphabet[::-1]

message = input('Введите строку: ').lower()

encrypted = ''

for i in message:
    for j, l in enumerate(alphabet):
        if i == l:
            encrypted = encrypted+alphabet_revers[j]

print('Криптограмма:', encrypted)
```

Контрольный пример

```
: # 1. Шифр Цезаря
```

```
: alphabet = 'абвгдежзийклмнопрстуфхцчшщыьэюя '
```

```
: message = input('Введите строку: ').lower()
  key = int(input('Введите ключ: '))
```

```
Введите строку: привет
Введите ключ: 4
```

```
: encrypted = ''
```

```
: for letter in message:
      if letter in alphabet:
          t = alphabet.find(letter)
          new_key = (t + key) % len(alphabet)
          encrypted += alphabet[new_key]
      else:
          encrypted += letter
```

```
: print('Криптограмма:', encrypted)
```

```
Криптограмма: уфмёиц
```

Пример работы алгоритма Цезаря

```
# 2. Шифр Атбаш
```

```
alphabet = 'абвгдежзийклмнопрстуфхцчшщыьэюя '
```

```
alphabet_revers= alphabet[::-1]
```

```
message = input('Введите строку: ').lower()
```

```
Введите строку: привет
```

```
encrypted = ''
```

```
for i in message:
    for j, l in enumerate(alphabet):
        if i == l:
            encrypted = encrypted+alphabet_revers[j]
```

```
print('Криптограмма:', encrypted)
```

```
Криптограмма: рпчюын
```

Пример работы алгоритма Атбаш

Выводы

В ходе выполнения работы удалось изучить шифры простой замены: шифр Цезаря и шифр Атбаш, а также реализовать данные алгоритм программно на языке Python.

Список литературы

1. Шифр Атбаш
2. Шифр Цезаря
3. Шифр Цезаря