Первая лабораторная работа. Шифры простой замены

НФИмд-01-23

Асеинова Елизавета Валерьевна

Содержание

Список таблиц

Список иллюстраций

1. Цель работы

Цель данной работы - ознакомиться с шифрами простой замены: шифр Цезаря и шифр Атбаш, а также научиться применять их на практике.

2. Задание

1. Реализовать шифр Цезаря с произвольным ключом k
2. Реализовать шифр Атбаш

3. Теоретическое введение

Шифр Цезаря - это моноалфавитная подстановка, т.е каждой букве открытого текста ставится в соответствие одна буква шифртекста. 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 вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

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

Атбаш — простой шифр подстановки для алфавитного письма. Правило шифрования состоит в замене i-й буквы алфавита буквой с номером n-i+1, где n — число букв в алфавите.

4. Выполнение лабораторной работы

1. Произведено ознакомление с шифрами Цезаря и Атбаш по методическим материалам курса

2. Прописан код для шифра Цезаря на языке программирования Python. Код для англоязычных сообщений. Сначала определяем, является ли символ буквой, затем проверяем на верхний и нижний регистр. После этого по формуле определяем символ, полученный в результате сдвига элемента на значение k. Символы, не являющиеся буквами, остаются неизменными.

```
def ceasar_cipher(text, k):
  result= ""

  for char in text:
    if char.isalpha():
      if char.isupper():
        alphabet_start = ord('A')
      else:
        alphabet_start = ord('a')

      shift_char = chr((ord(char) - alphabet_start + k) % 26 + alphabet_start)

      result += shift_char

    else:
      result += char

  return result
```

Рис. 4.1.: Шифр Цезаря

3. Выводим на экран результат применения шифра Цезаря для произвольного текста со сдвигом на значение k = 5.

```
[10] text = input ("Введите текст для шифрования на английском языке: ")
     k = int(input("Введите значение сдвига: "))

     encrypted_text = ceasar_cipher(text, k)
     print("Зашифрованный текст: ", encrypted_text)

     Введите текст для шифрования на английском языке: Hello, my name is Liza!
     Введите значение сдвига: 5
     Зашифрованный текст:  Mjqqt, rd sfrj nx Qnef!
```

Рис. 4.2.: Результат применения шифра Цезаря

4. Прописан код для шифра Атбаш на языке программирования Python. Код для англоязычных сообщений. Сначала определяем, является ли символ буквой, затем проверяем на верхний и нижний регистр. После этого по формуле определяем символ, полученный в результате отзеркаливание элемента. Символы, не являющиеся буквами, остаются неизменными.

```
[11] def atbash_cipher(text):
       result= ""

       for char in text:
         if char.isalpha():
           if char.isupper():
             alphabet_start = ord('A')
             alphabet_end = ord('Z')
           else:
             alphabet_start = ord('a')
             alphabet_end = ord('z')

           reverse_char = chr(alphabet_end - (ord(char) - alphabet_start))

           result += reverse_char

         else:
           result += char

       return result
```

Рис. 4.3.: Шифр Атбаш

5. Выводим на экран результат применения шифра Атбаш.

```
[10] text = input ("Введите текст для шифрования на английском языке: ")
     k = int(input("Введите значение сдвига: "))

     encrypted_text = ceasar_cipher(text, k)
     print("Зашифрованный текст: ", encrypted_text)

     Введите текст для шифрования на английском языке: Hello, my name is Liza!
     Введите значение сдвига: 5
     Зашифрованный текст:  Mjqqt, rd sfrj nx Qnef!
```

Рис. 4.4.: Результат применения шифра Атбаш

5. Выводы

В рамках данной лабораторной работы было произведено ознакомление с шифром Цезаря и шифром Атбаш. Оба шифра были реализованы на языке программирования Python.

6. Список литературы

1. Методические материалы курса