Отчёт по лабораторной работе 1

Шифры простой замены

Гебриал Ибрам Есам Зекри НФИ-02-22

Содержание

List of Tables

List of Figures

1 Цель работы

Приобретение навыков программной реализации простых шифров подстановки и замены.

2 Теоретические сведения

Шифр Цезаря (также он является шифром простой замены) - это моноалфавитная подстановка, т.е. каждой букве открытого текста ставится в соответствие одна буква шифртекста. На практике при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит, но с нарушенным порядком букв алфавитная перестановка).

При достижении конца алфавита выполнялся циклический переход к его началу. Таким образом, шифр-алфавит циклически сдвинут влево на K позиций относительно нормативного алфавита.

Цезарь использовал этот шифр замены при смещении. k = 3. Такой шифр можно задать таблицей подстановок, содержащей соответствующие пары букв открытого текста и шифротекста [1]. (рис. 2.1)

Порядковый номер символа	0	1	2	3	4		23	24	25
Нормативный алфавит	a	b	c	d	e		x	y	z
	↓	↓	↓	↓	↓	...	↓	↓	↓
Алфавит шифрования	d	e	f	g	h		a	b	c
Порядковый номер символа	3	4	5	6	7		0	1	2

Figure 2.1: Шифр Цезаря

Шифр Атбаш:

Еще один шифр простой (моноалфавитной) замены. Шифрование осуществляется путем замены первой буквы алфавита на последнюю, второй на предпоследнюю и так далее. (рис. 2.2)

Этот шифр использовался для еврейского алфавита и отсюда получил свое название. Первая буква - алеф, заменяется на тау (последнюю), вторая буква - бет,

заменяется на шин (предпоследнюю). Из этих букв и сформировалось название.

[]

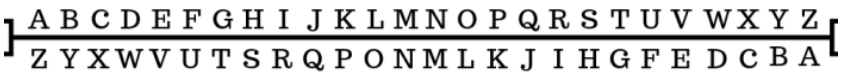

Figure 2.2: Шифр Атбаш

3 Выполнение лабораторной работы

1. Написал функцию caesar для шифрования и расшифровки текста. (рис. 3.1)

Сначала написал алфавит в виде списки.

Для расшифровки умножил ключ на -1.

Написал цикл для проверки каждой буквы в нашем слове, а затем определил ее позицию в алфавите с помощью index метода, который возвращает индекс указанного элемента в списке. Как определил позицию, сложил на него ключ (shift). потом распечатал зашифрованный текст.

```
alphabet = ['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h',
'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r',
's', 't', 'u', 'v', 'w', 'x', 'y', 'z', 'a', 'b',
'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l',
'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v',
'w', 'x', 'y', 'z']

def caesar(start, shift, direction):
  end_text = ""
  if direction == "decode":
    shift *= -1
  for char in start:
    if char in alphabet:
      position = alphabet.index(char)
      new_position = (position + shift) % 26
      end_text += alphabet[new_position]
    else:
      end_text += char
  print(f"Here's the {direction}d result:
{end_text}")
```

Figure 3.1: Функция для кодирования текста шифром Цезаря

2. Написал функцию atbash для шифрования и расшифровки текста. (рис. 3.2)

Для атбаша сделал аналогично, для сдвига на всю длину алфавита нам нужно умножить позицию на -1.

```
15
16 def atbash (start):
17     end_text = ""
18     for char in start:
19         if char in alphabet:
20             position = alphabet.index(char)+1
21             end_text += alphabet[position*(-1)]
22         else:
23             end_text += char
24
25     print(f"Here's the atbash result: {end_text}")
26
```

Figure 3.2: Функция для кодирования текста шифром Атбаша

3. Написал блок выбора нужного метода и ввода текста. (рис. 3.3)

```
27 should_continue = True
28 while should_continue:
29   cipher= input("Type 'caesar' to use caesar cipher,
   type 'atbash'  to use atbash cipher:\n")
30   text = input("Type your message:\n").lower()
31
32   if cipher == "caesar":
33     direction = input("Type 'encode' to encrypt,
   type 'decode' to decrypt:\n")
34     shift = int(input("Type the shift number:\n"))
35     shift = shift % 26
36     caesar(start=text, shift=shift,
   direction=direction)
37
38   else:
39     atbash(start=text)
40
41   restart = input("Type 'yes' if you want to go
   again. Otherwise type 'no'.\n")
42   if restart == "no":
43     should_continue = False
44     print("Goodbye")
45
```

Figure 3.3: Код для выбора метод шифрования и ввода текста

4. Зашифровал и расшифровал слова Hello с помощью шифра Цезаря. (рис. 3.4)

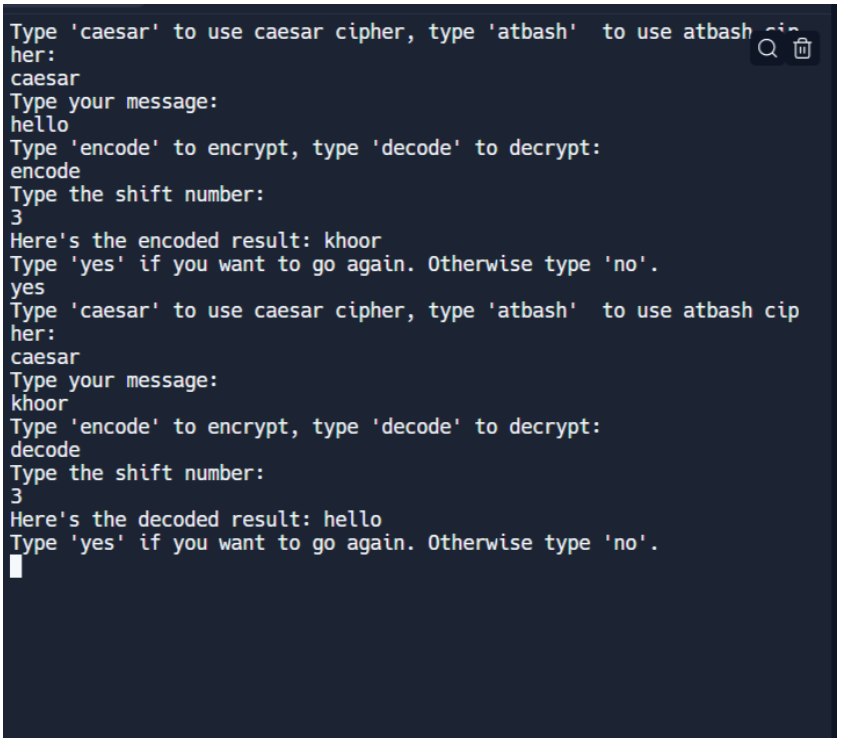

Figure 3.4: Получение шифрования и расшифровки текста методом Цезаря

5. Зашифровал и расшифровал слова Hello с помощью Атбаша. (рис. 3.5)

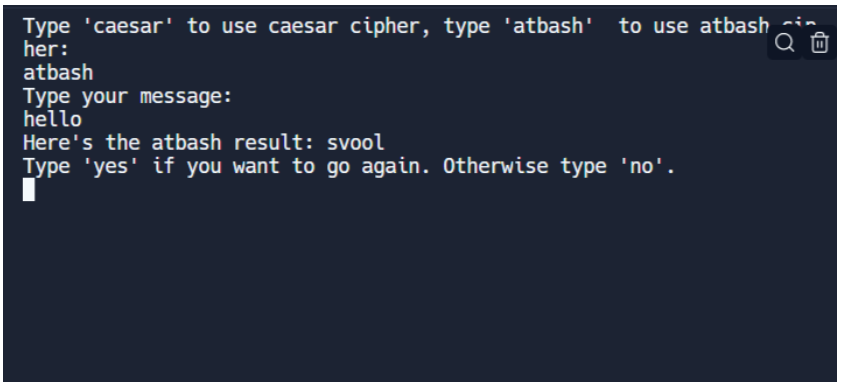

Figure 3.5: Получение шифрования текста методом Атбаша

4 Выводы

Приобрел навыки программной реализации простых шифров подстановки и замены.

5 Список литературы

1. Шифры простой замены. — URL: https://studme.org/239550/informatika/shifry_prostoy_zameny.
2. Шифр Атбаш. — URL: https://studbooks.net/2215784/informatika/shifr_atbash.