

Математические основы защиты информации и информационной безопасности.

Лабораторная работа №1.

Сапёров Максим Александрович.

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	10

List of Figures

3.1	Caesar cipher	7
3.2	Caesar decipher	7
3.3	Atbash cipher	8
3.4	Atbash decipher	8
3.5	tests	9

List of Tables

1 Цель работы

Освоить на практике шифрование шифров Цезаря и Атбаша.

2 Задание

1. Реализовать шифр Цезаря
2. Реализовать шифр Атбаш

3 Выполнение лабораторной работы

Написал код для зашивровки кодов шифром Цезаря

```
✓ [46] def caesar_chipper(text, k):  
0s      result = ''  
      for letter in text:  
          if not(letter.isalpha()):  
              result+=letter  
          else:  
              if letter.isupper():  
                  result+=(chr((ord(letter)+k-65)%26+65))  
              else:  
                  result+=(chr((ord(letter)+k-97)%26+97))  
      return result
```

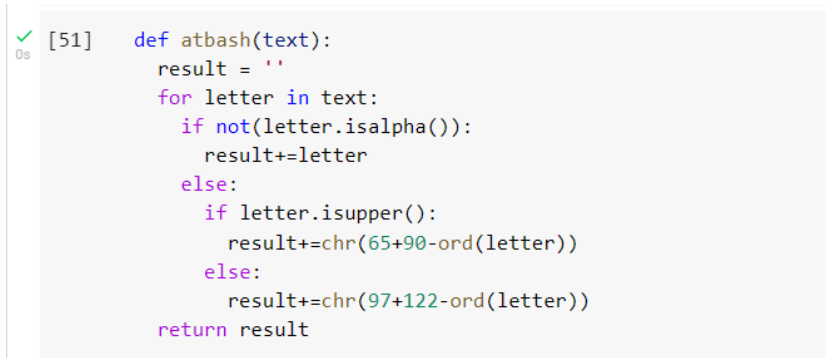
Figure 3.1: Caesar cipher

Написал код для дешифровки кодов шифром Цезаря

```
✓ [47] def caesar_dechipper(text, k):  
0s      result = ''  
      for letter in text:  
          if not(letter.isalpha()):  
              result+=letter  
          else:  
              if letter.isupper():  
                  result+=(chr((ord(letter)-k-65)%26+65))  
              else:  
                  result+=(chr((ord(letter)-k-97)%26+97))  
      return result
```

Figure 3.2: Caesar decipher

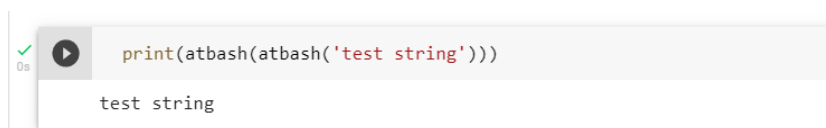
Написал код для зашивровки кодов шифром Атбаша

A screenshot of a code editor showing a Python function named 'atbash'. The function takes a string 'text' as input and returns a new string 'result'. It iterates through each 'letter' in 'text'. If the letter is not an alpha character, it is added to 'result' as-is. If it is an alpha character, it is converted to its Atbash equivalent using ASCII values: uppercase letters are mapped to uppercase letters (e.g., 'A' to 'Z'), and lowercase letters are mapped to lowercase letters (e.g., 'a' to 'z').

```
[51] def atbash(text):  
    result = ''  
    for letter in text:  
        if not(letter.isalpha()):  
            result+=letter  
        else:  
            if letter.isupper():  
                result+=chr(65+90-ord(letter))  
            else:  
                result+=chr(97+122-ord(letter))  
    return result
```

Figure 3.3: Atbash cipher

Для дешифровки кодов шифром Атбаша можно повторно использовать ту же функцию, что и для зашифровки

A screenshot of a code editor showing a single line of Python code that prints the result of applying the 'atbash' function twice to the string 'test string'. Below the code, the output 'test string' is displayed.

```
print(atbash(atbash('test string')))
```

test string

Figure 3.4: Atbash decipher

Результаты тестов. Первые три строчки это зашифрованные сообщения шифром Цезаря. Следующие три строчки, это расшифрованные сообщения. Следующие три строчки, это те же сообщения, но зашифрованные шифром Атбаш. И последние три строчки — расшифрованные сообщения.


```
print(f'''
Цезарь шифр:
{caesar_chipper(test1,3)},
{caesar_chipper(test2,3)},
{caesar_chipper(test3,3)},

Цезарь расшифровка:
{caesar_dechipper(caesar_chipper(test1,3),3)},
{caesar_dechipper(caesar_chipper(test2,3),3)},
{caesar_dechipper(caesar_chipper(test3,3),3)},

Атбаш шифр:
{atbash(test1)},
{atbash(test2)},
{atbash(test3)},

Атбаш расшифровка:
{atbash(atbash(test1))},
{atbash(atbash(test2))},
{atbash(atbash(test3))}
...
''')

Цезарь шифр:
Yhql, Yhgl, Ylfl,
Phqlqur prul,
Gxp Vslur, Vshur,

Цезарь расшифровка:
Venl, Vedi, Vici,
Memento mori,
Dum Spiro, Spero,

Атбаш шифр:
Evmr, Evnr, Erxr,
Nvnvmgl nlin,
Wfn Hkril, Hkvil,

Атбаш расшифровка:
Venl, Vedi, Vici,
Memento mori,
Dum Spiro, Spero
```

Figure 3.5: tests

4 Выводы

Освоил на практике применение методов шифрования Цезаря и Атбаша.