

Отчёт по лабораторной работе №1

Шифр простой замены

Мадаманов Аллаберды

Содержание

Цель работы	4
Теоретические сведения	5
Шифр Цезаря	5
Шифр Атбаш	6
Выполнение работы	7
Реализация шифра Цезаря на языке Python	7
Реализация шифра Атбаш на языке Python	8
Пример работы	9
Выводы	10

Список иллюстраций

1	Работа алгоритмов	9
---	-----------------------------	---

Цель работы

Изучение алгоритмов шифрования Цезаря и Атбаш

Теоретические сведения

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, 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:

$$y = (x + k) \bmod n$$

$$x = (y - k + n) \bmod n$$

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

С точки зрения математики шифр Цезаря является частным случаем аффинного шифра.

Шифр Атбаш

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

Выполнение работы

Реализация шифра Цезаря на языке Python

Блок шифрования

```
def caesar():

    letters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'

    step = 5
    text = input("Шифрование Цезаря")
    result = ''
    for i in text:
        ind = letters.find(i)
        newind = ind + step
        if i in letters:
            result += letters[newind]
        else:
            result += i
    print(result)
```

Блок дешифровки

```
def caesar_deshifr():
```

```

letters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'
smeshenie = 5
text = input("Дешифровка Цезарь")
result = ''

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

```

Реализация шифра Атбаш на языке Python

Блок шифрования

```

def atbash():
    letters = [chr(x) for x in range(65, 91)]
    letters_r = [x for x in letters]
    letters_r.reverse()

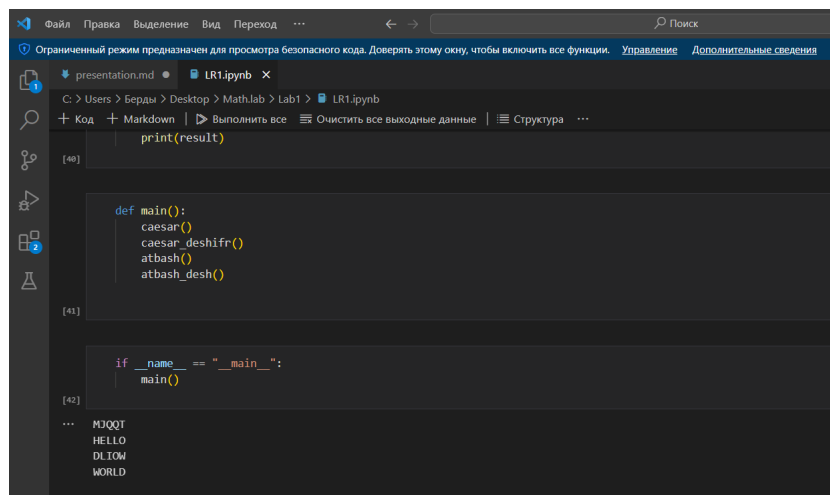
    text = input("Шифрование Атбаш")
    result = ""
    for i in text:
        for j,l in enumerate(letters):
            if i == l:
                result += letters_r[j]
    print(result)

```


Блок дешифровки

```
def atbash_desh():  
    letters = [chr(x) for x in range(65, 91)]  
    letters_r = [x for x in letters]  
    letters_r.reverse()  
  
    text = input("Дешифровка Атбаш")  
    result = ""  
    for i in text:  
        for j, l in enumerate(letters_r):  
            if i == l:  
                result += letters[j]  
    print(result)
```

Пример работы



The screenshot shows a Jupyter Notebook window with the following content:

- File Explorer:** Shows the file path `C:\Users\Берды\Desktop\Mathlab\Lab1\LR1.ipynb`.
- Code Editor:** Contains the following Python code:

```
def main():  
    caesar()  
    caesar_deshifr()  
    atbash()  
    atbash_desh()  
  
if __name__ == "__main__":  
    main()
```
- Output:** The output of the `atbash_desh()` function is displayed as:

```
...  
MJJQT  
HELLO  
DLIOM  
WORLD
```

Рис. 1: Работа алгоритмов

Выводы

В данной работе мы изучили алгоритмы шифрования Цезаря и Атбаш.