

Шифр простой замены

Мадаманов Аллаберды

4 февраля, 2024, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритмов шифрования Цезаря и Атбаш

Выполнение лабораторной работы

Шифрование – это такое преобразование исходного сообщения, которое не позволит всяким нехорошим людям прочесть данные, если они это сообщение перехватят. Делается это преобразование по специальным математическим и логическим алгоритмам.

Атбаш — простой шифр подстановки.

Правило шифрования состоит в замене i -й буквы алфавита буквой с номером $n - i + 1$, где n — число букв в алфавите.

Шифр Цезаря

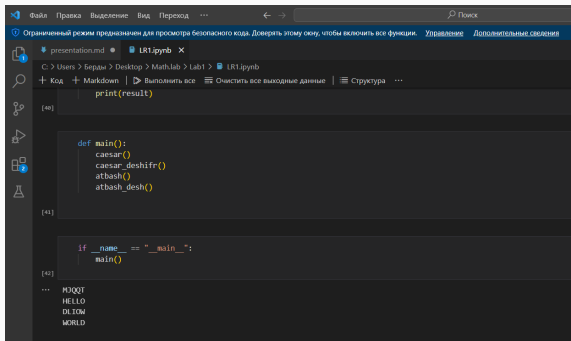
Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом 3 А была бы заменена на Г, Б станет Д, и так далее.

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

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

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

Пример



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

```
presentation.mdx LR1.ipynb X
C:\Users\Беран\Desktop\MathLab\Lab1> LR1.ipynb
+ Код + Markdown | ▶ Выполнить все | Очистить все выходные данные | Структура ...

[40]
print(result)

[41]
def main():
    caesar()
    caesar_deshifr()
    atbash()
    atbash_desh()

[42]
if __name__ == "__main__":
    main()

...
HQQQT
HELLO
DLTOW
WORLD
```

Рис. 1: Работа алгоритмов

Выводы

В данной работе мы изучили алгоритмы шифрования Цезаря и Атбаш.