
Front matter

lang: ru-RU title: Шифр простой замены author: Мадаманов Аллаберды institute: Российский Университет Дружбы Народов date:4 февраля, 2024, Москва, Россия

Formatting

mainfont: PT Serif romanfont: PT Serif sansfont: PT Sans monofont: PT Mono toc: false slide_level: 2 theme: metropolis header-includes:

- \metroset{progressbar=frametitle,sectionpage=progressbar,numbering=fraction}
- '\makeatletter'
- '\beamer@ignorenonframefalse'
- '\makeatother' aspectratio: 43 section-titles: true

Цели и задачи

Цель лабораторной работы

Изучение алгоритмов шифрования Цезаря и Атбаш

Выполнение лабораторной работы

Шифрование

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.

Шифр Атбаш

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.

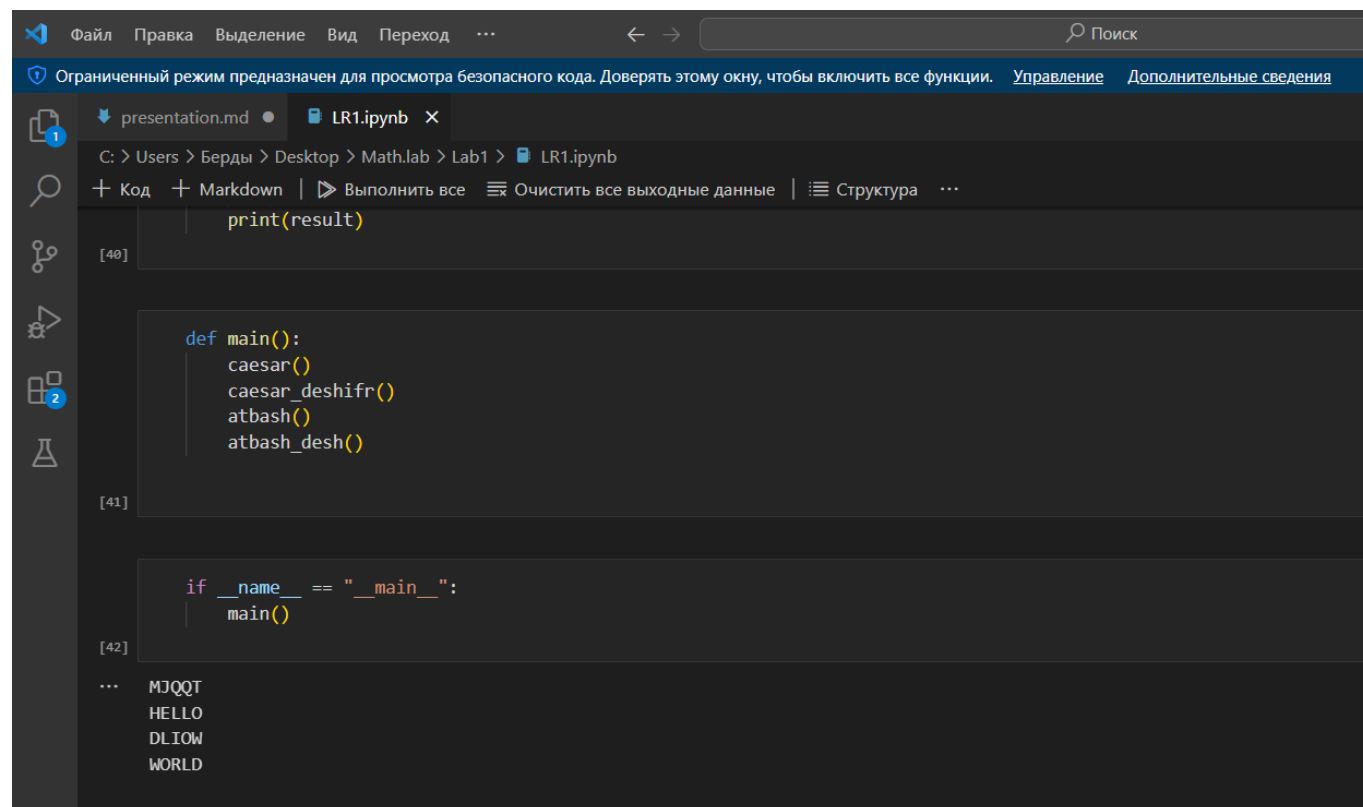
Шифр Цезаря

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 titled 'LR1.ipynb'. The interface includes a menu bar with options like 'Файл', 'Правка', 'Выделение', 'Вид', 'Переход', and 'Поиск'. Below the menu bar, there is a status bar indicating 'Ограниченный режим предназначен для просмотра безопасного кода. Доверять этому окну, чтобы включить все функции.' The notebook content is divided into three cells. The first cell contains the code `print(result)`. The second cell contains a function definition `def main():` with sub-calls `caesar()`, `caesar_deshifr()`, `atbash()`, and `atbash_desh()`. The third cell contains a conditional execution block `if __name__ == "__main__":` followed by `main()`. The output of the notebook shows the results of the encryption and decryption processes, including the original text 'HELLO' and 'WORLD' and their encrypted/decrypted versions.

```
print(result)
```

```
def main():
    caesar()
    caesar_deshifr()
    atbash()
    atbash_desh()
```

```
if __name__ == "__main__":
    main()
```

```
... MJQQT
    HELLO
    DLIOW
    WORLD
```

{ #fig:001 width=70% height=70%}

Выводы

Результаты выполнения лабораторной работы

В данной работе мы изучили алгоритмы шифрования Цезаря и Атбаш.