Математические основы защиты информации и информационной безопасности. Лабораторная работа № 1 на тему “Шифры простой замены”

Лубышева Ярослава Михайловна

RUDN University, Moscow, Russian Federation

Содержание

Содержание

Прагматика

Прагматика

Шифр Цезаря, также известный как шифр сдвига, код Цезаря — один из самых простых и наиболее широко известных методов шифрования. 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 вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Прагматика

Шифр Атбаш является шифром сдвига на всю длину алфавита. Для алфавита, состоящего только из русских букв и пробела, будет иметь следущи вид:

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я -

- Я Ю Э Ь Ы Ъ Щ Ш Ч Ц Х Ф У Т С Р П О Н М Л К Й И З Ж Е Д Г В Б А

Цели и задачи

Цели и задачи

Выполнить задание к лабораторной работе № 1 [1]

Выполнение

Выполнение

```python
# 1) реализовать шифр Цезаря с произволным ключом k

k = 3   # ключ
# алфавит
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']
# разер алфавита
alp_size = len(alphabet)

mes = input("Enter the message to encrypt: ").upper()
print(mes)

for a in mes:
    if a == ' ':
        print(a, end='')
    else:
        i = alphabet.index(a)   # индекс буквы в алфавите
        j = (i+k)%alp_size     # индекс буквы-шифра
        print(alphabet[j], end='')
```

Figure 1: Реализация шифра Цезаря

Выполнение

```
Enter the message to encrypt: Veni vidi vici
VENI VIDI VICI
YHQL YLGL YLFL
```

Figure 2: Результат работы программы для шифра Цезаря

Выполнение

```python
# 2) реализовать шифр Атбаш

# алфавит
alphabet = ['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п',
            'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ъ', 'ы', 'ь', 'э', 'ю', 'я', ' ']
# алфавит-шифр
alphabet_code = alphabet.copy()
alphabet_code.reverse()

mes = input("Enter the message to encrypt: ").lower()
print(mes)

for a in mes:
    i = alphabet.index(a)  # индекс буквы в алфавите
    print(alphabet_code[i], end='')
```

Figure 3: Реализация шифра Атбаш

Выполнение

```
Enter the message to encrypt: Привет МИР
привет мир
сршюыоафшр
```

Figure 4: Результат работы программы для шифра Атбаш

Результаты

Результаты

Выполнено задание к лабораторной работе № 1

Список литературы

Список литературы

1. Методические материалы курса