

# **Информационная безопасность. Отчет по лабораторной работе №**

Тема

Горбунова Ярослава Михайловна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
<b>5</b>	<b>Выводы</b>	<b>10</b>
<b>6</b>	<b>Список литературы</b>	<b>11</b>

# List of Figures

4.1	Реализация шифра Цезаря . . . . .	8
4.2	Результат работы программы для шифра Цезаря . . . . .	9
4.3	Реализация шифра Атбаш . . . . .	9
4.4	Результат работы программы для шифра Атбаш . . . . .	9

## List of Tables

# **1 Цель работы**

Выполнить задание к лабораторной работе № 1 [1].

## 2 Задание

1. Реализовать шифр Цезаря с произвольным ключом  $k$ .
2. Реализовать шифр Атбаш.

### 3 Теоретическое введение

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.

Шифр Атбаш является шифром сдвига на всю длину алфавита. Для алфавита, состоящего только из русских букв и пробела, будет иметь следующий 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 ъ ы ь 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

## 4 Выполнение лабораторной работы

Для реализации шифра Цезаря была написана следующая программа на языке программирования Python (fig. 4.1).

```
1  # 1) реализовать шифр Цезаря с произвольным ключом k
2
3  k = 3 # ключ
4  # алфавит
5  alphabet = ['A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M',
6             'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']
7  # размер алфавита
8  alp_size = len(alphabet)
9
10 mes = input("Enter the message to encrypt: ").upper()
11 print(mes)
12
13 for a in mes:
14     if a == ' ':
15         print(a, end='')
16     else:
17         i = alphabet.index(a) # индекс буквы в алфавите
18         j = (i+k)%alp_size    # индекс буквы-шифра
19         print(alphabet[j], end='')

```

Figure 4.1: Реализация шифра Цезаря

Результаты работы программы представлены на следующем рисунке (fig. 4.2).



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

Figure 4.2: Результат работы программы для шифра Цезаря

Для реализации шифра Атбаш также была написана программа на языке программирования Python (fig. 4.3).

```
1  # 2) реализовать шифр Атбаш  
2  
3  # алфавит  
4  alphabet = ['a', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п',  
5             'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ъ', 'ы', 'ь', 'э', 'ю', 'я', ' ']  
6  # алфавит-шифр  
7  alphabet_code = alphabet.copy()  
8  alphabet_code.reverse()  
9  
10 mes = input("Enter the message to encrypt: ").lower()  
11 print(mes)  
12  
13 for a in mes:  
14     i = alphabet.index(a) # индекс буквы в алфавите  
15     print(alphabet_code[i], end='')
```

Figure 4.3: Реализация шифра Атбаш

Результаты работы программы представлены на рисунке ниже (fig. 4.4).

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

Figure 4.4: Результат работы программы для шифра Атбаш

## **5 Выводы**

Выполнено задание к лабораторной работе № 1.

## **6 Список литературы**

1. Методические материалы курса