Информационная безопасность. Отчет по лабораторной работе №

Тема

Горбунова Ярослава Михайловна

Содержание

# 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 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

# 4 Выполнение лабораторной работы

Для реализации шифра Цезаря была написана следующая программа на языке программирования Python (fig. 1).

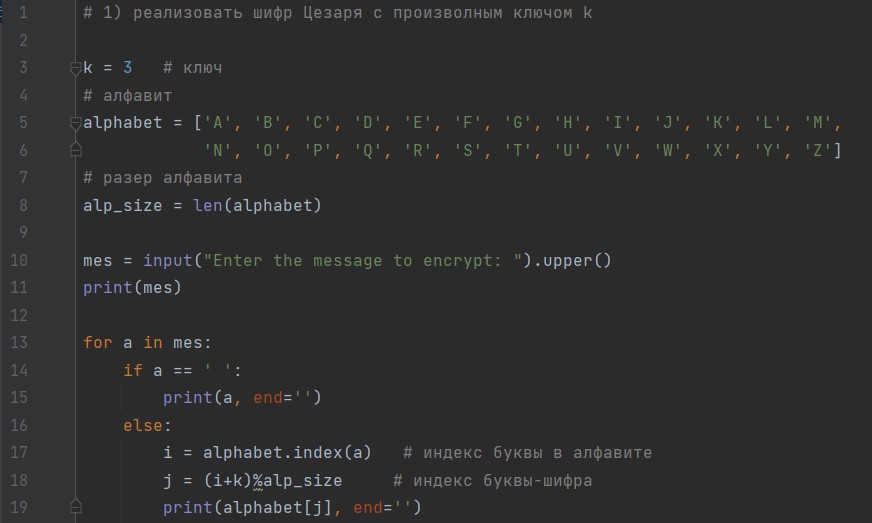


Figure 1: Реализация шифра Цезаря

Результаты работы программы представлены на следующем рисунке (fig. 2).

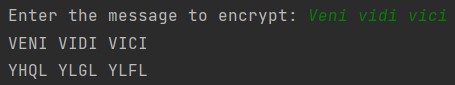


Figure 2: Результат работы программы для шифра Цезаря

Для реализации шифра Атбаш также была написана программа на языке программирования Python (fig. 3).

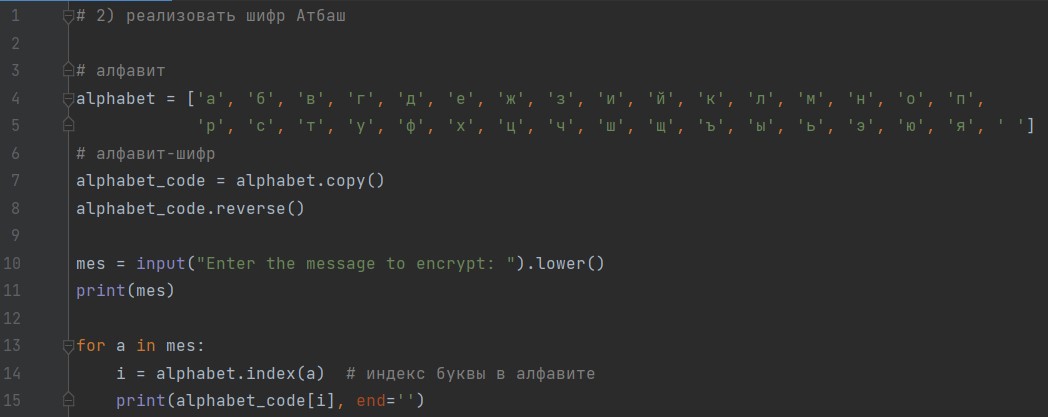


Figure 3: Реализация шифра Атбаш

Результаты работы программы представлены на рисунке ниже (fig. 4).

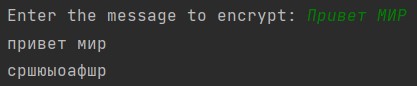


Figure 4: Результат работы программы для шифра Атбаш

# 5 Выводы

Выполнено задание к лабораторной работе № 1.

# 6 Список литературы

1. Методические материалы курса