Лабораторная работа №1

Математические основы защиты информации и информационной безопасности

Минов Кирилл Вячеславович| НПМмд-02-23

Содержание

# 1 Цель работы

Реализовать на языке программирования шифр Цезаря с произвольным ключом k и шифр Атбаш.

# 2 Теоретическое введение

Шифр Цезаря (шифр простой замены) - это моноалфавитная подстановка, т.е. каждой букве открытого текста ставится в соответствие одна буква шифртекста. На практике при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит, но с нарушенным порядком букв (алфавитная перестановка).

Математически процедуру шифрования можно описать следующим образом: , где - операция нахождения остатка от целочисленного деления на , а - циклическая группа. Обобщение шифра Цезаря на случай произвольного ключа k для латинского алфавита: .

Шифр Атбаш является шифром сдвига на всю длину алфавита. Для реализации шифра целесообразно пользоваться таблицей ASCII и функциями работы с ней: ord и char.

# 3 Выполнение лабораторной работы

Первым заданием был шифр Цезаря. Переменные message и offset соответсвуют введеными с клавиатуры тексту и ключу, нужному для шифрования. result - конечное представления введенного текста. originalAlphabetPosition - переменная, в которой лежит изначальное положение элемента, newAlphabetPosition - позиция элемента после примнения шифрования. newCharacter - переменная отвечающая за хранения полученного элемента после шифровки. Весь алгоритм представляет из себя цикл в котором мы вычисляем текущее положение, новое положение и новую букву.

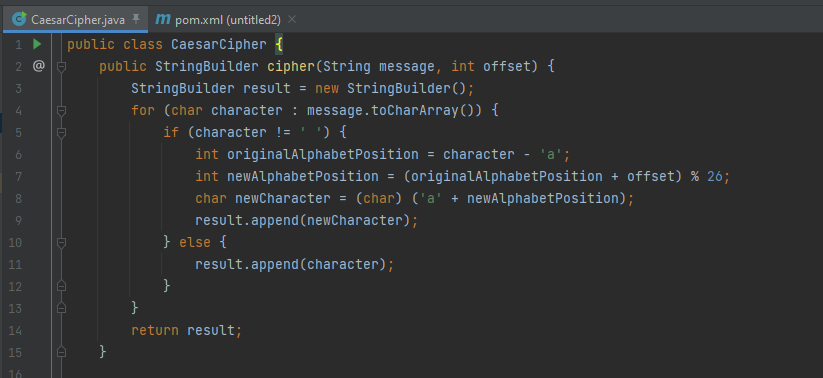


Рис.1 (Реализация шифра Цезаря)



Рис.2 (Пример работы)

Второе задание - реализация шифра Атбаш. Создание пустой строки ciphertext для хранения зашифрованного текста.

Проход по каждому символу в исходном тексте plaintext с помощью цикла for. Для каждого символа в plaintext:

Проверка, является ли символ буквой с помощью Character.isLetter(currentChar). Если символ не является буквой, он остается без изменений, и мы добавляем его к ciphertext. Если символ - буква, мы определяем, является ли она заглавной или строчной буквой, сравнивая её с символом 'A'. Если символ в верхнем регистре, baseChar устанавливается как 'A', иначе как 'a'. Мы вычисляем смещение offset текущей буквы относительно baseChar. Например, для буквы 'c' смещение составит 2 (поскольку 'c' идет после 'a' и 'b' в алфавите). Мы находим зашифрованную букву, вычитая offset из индекса текущей буквы относительно baseChar и добавляя это значение к baseChar. Например, если текущая буква - 'c', то зашифрованная буква будет 'x'. Зашифрованная буква добавляется к строке ciphertext. По завершении цикла, строка ciphertext содержит зашифрованный текст, и он возвращается как результат работы метода encrypt.

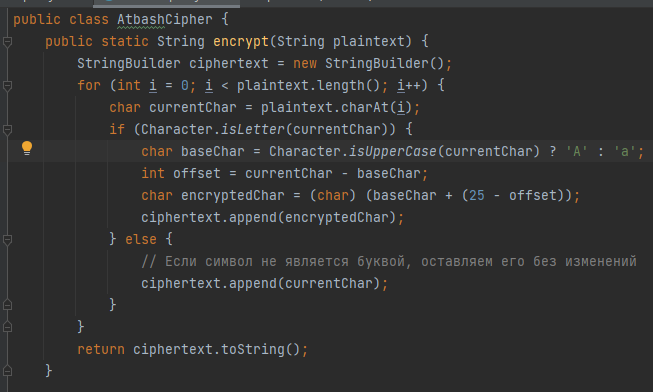


Рис.3(Реализация шифра)

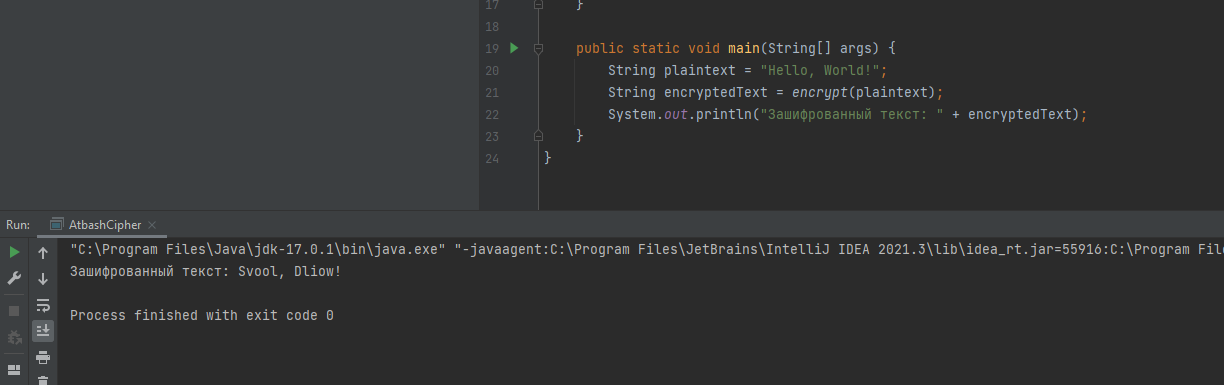


Рис.4(Пример работы)

# 4 Выводы

В ходе выполнения данной лабораторной работы были реализованы шифры Цезаря и Атбаш на языке программирования Java.

# Список литературы

1. Шифр Цезаря [Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F>.

2. Шифр Атбаш [Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B1%D0%B0%D1%88>