

Лабораторная работа №1

Математические основы защиты информации и информационной безопасности

- Минов Кирилл Вячеславович
- 23.09.2023
- Российский университет дружбы народов
- Россия, Москва

Цель лабораторной работы

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

Задачи лабораторной работы

1. Изучить теоретическую часть лабораторной работы по методичке
2. Написать соответствующие программы

Теоретическое введение

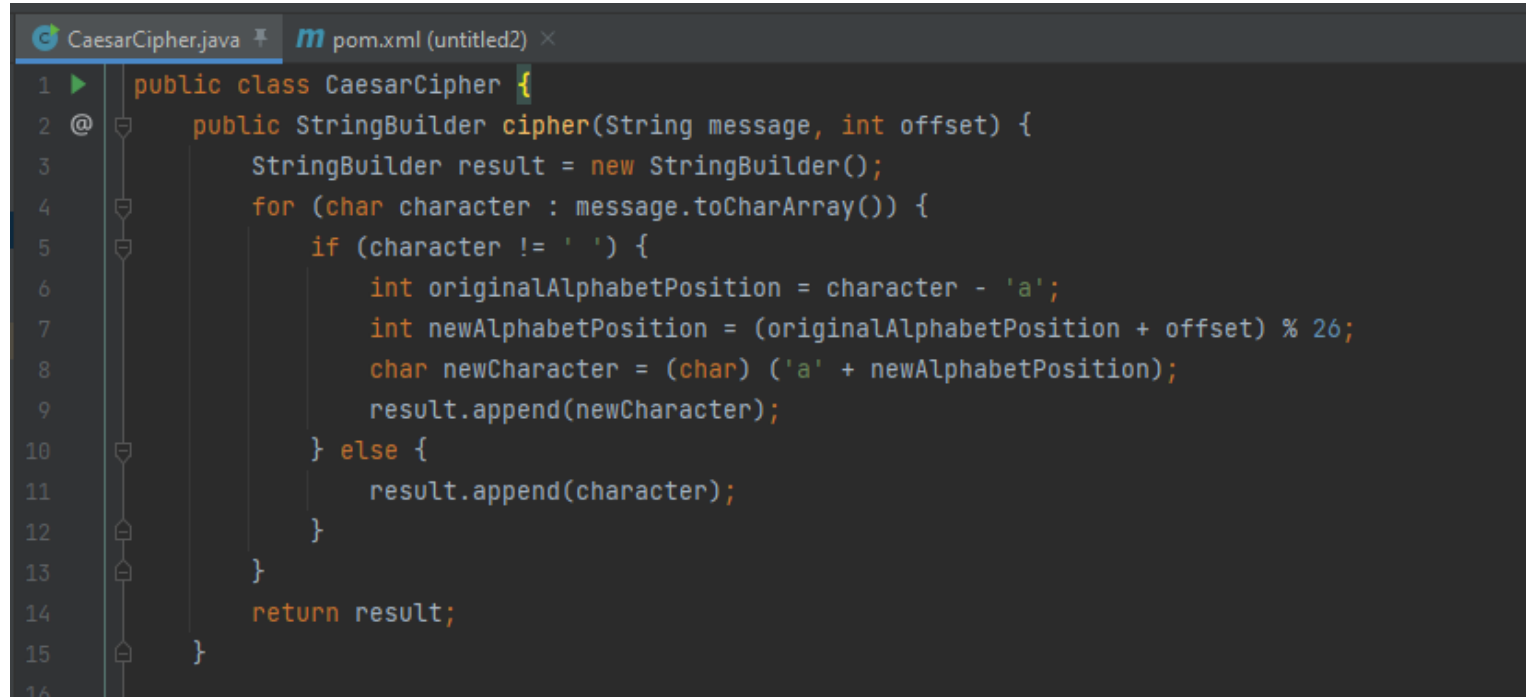
- **Шифр Цезаря** (является шифром простой замены) - это моноалфавитная подстановка, т.е. каждой букве открытого текста ставится в соответствие одна буква шифртекста. На практике при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит, но с нарушенным порядком букв.

Теоретическое введение

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

Ход выполнения лабораторной работы

Реализация шифра
Цезаря



```
CaesarCipher.java pom.xml (untitled2) x
1 public class CaesarCipher {
2     @ public StringBuilder cipher(String message, int offset) {
3         StringBuilder result = new StringBuilder();
4         for (char character : message.toCharArray()) {
5             if (character != ' ') {
6                 int originalAlphabetPosition = character - 'a';
7                 int newAlphabetPosition = (originalAlphabetPosition + offset) % 26;
8                 char newCharacter = (char) ('a' + newAlphabetPosition);
9                 result.append(newCharacter);
10            } else {
11                result.append(character);
12            }
13        }
14        return result;
15    }
16 }
```

```
public class AtbashCipher {  
    public static String encrypt(String plaintext) {  
        StringBuilder ciphertext = new StringBuilder();  
        for (int i = 0; i < plaintext.length(); i++) {  
            char currentChar = plaintext.charAt(i);  
            if (Character.isLetter(currentChar)) {  
                char baseChar = Character.isUpperCase(currentChar) ? 'A' : 'a';  
                int offset = currentChar - baseChar;  
                char encryptedChar = (char) (baseChar + (25 - offset));  
                ciphertext.append(encryptedChar);  
            } else {  
                // Если символ не является буквой, оставляем его без изменений  
                ciphertext.append(currentChar);  
            }  
        }  
        return ciphertext.toString();  
    }  
}
```

Ход выполнения лабораторной работы

Реализация шифра Атбаш

Вывод

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