

Лабораторная работа №1

Шифры простой замены

Топонен Н. А.

18 сентября 2023

Российский университет дружбы народов, Москва, Россия

Информация

- Топонен Никита Андреевич
- студент Российского университет дружбы народов
- 1132236933@rudn.ru
- <https://github.com/natoponen>



Вводная часть

- Познакомиться с шифрами простой замены
- Реализовать шифр Цезаря
- Реализовать шифр Атбаш

- Реализовать шифр Цезаря с произвольным ключом k .
- Реализовать шифр Атбаш.

Теоретическое введение

- Шифр Цезаря — 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 — простой шифр подстановки для алфавитного письма.
- Правило шифрования состоит в замене i -й буквы алфавита буквой с номером $n - i + 1$, где n — число букв в алфавите.

Выполнение лабораторной работы

```
for (char character : message.toCharArray()) {  
    if (character != ' ') {  
        // ASCII код буквы - ASCII код a  
        int originalAlphabetPosition = character - 'a';  
        // Находим смещение в зависимости от offset  
        int newAlphabetPosition =  
            (originalAlphabetPosition + offset) % 26;  
        // Достаем символ ASCII, прибавляя смещение  
        char newCharacter = (char) ('a' + newAlphabetPosition);  
        result.append(newCharacter);  
    } else {  
        result.append(character);  
    }  
}
```

```
C:\Users\Toponen\.jdk\openjdk-19.0.1\bin\java.exe "-javaagent:C:\Program FiT
Encoded message: fkhfnlqj wkh fhvdu frgh rq uhdo hadpsoh
Decoded message: checking the cesar code on real example

Process finished with exit code 0
```

Рис. 1: Результаты работы программы

```
private static final HashMap<Character, Character> ATBASH_TABLE =  
    new HashMap<>(){  
        put('a', 'z'); put('b', 'y'); put('c', 'x'); put('d', 'w');  
        put('e', 'v'); put('f', 'u'); put('g', 't'); put('h', 's');  
        put('i', 'r'); put('j', 'q'); put('k', 'p'); put('l', 'o');  
        put('m', 'n'); put('n', 'm'); put('o', 'l'); put('p', 'k');  
        put('q', 'j'); put('r', 'i'); put('s', 'h'); put('t', 'g');  
        put('u', 'f'); put('v', 'e'); put('w', 'd'); put('x', 'c');  
        put('y', 'b'); put('z', 'a');  
    };
```

```
public static String atbash(String message)
{
    StringBuilder result = new StringBuilder();

    for(char letter : message.toCharArray()) {
        result
            .append(Character
                .toLowerCase(ATBASH_TABLE.get(letter)));
    }

    return result.toString();
}
```

```
C:\Users\Toponen\.jdk\openjdk-19.0.1\bin\java.exe "-javaagent:  
Encoded message: ytwyqsnuahwa hz itaymxwamnajw pawd olpw  
Decoded message: checking the atbash code on real example  
  
Process finished with exit code 0
```

Рис. 2: Результаты работы программы

- Познакомился с шифрами простой замены
- Реализовал шифр Цезаря с произвольным ключом
- Реализовал шифр Атбаш