**Имена:** Венцислав Вълков

**Дата: 2015-06-04 Предмет: Програмиране с Java, част 1**

**email: vylkoff@abv.bg GitHub:** [**https://github.com/Vylkoff**](https://github.com/Vylkoff)

Шифриране и дешифриране на Цезар шифър

**1. Условие**

Програма, която шифрира и дешифрира въведен от потребителя текст и посредством зададено от потребителя отместване, се получава шифриран или дешифриран текст в зависимост от желанието на потребителя.

**2. Въведение**

Приложението е реализирано на Java платформа.

**3. Теория**

Шифърът на Цезар е вид [шифър](http://bg.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%8A%D1%80) с пряка субституция (*субституционен шифър*) - това означава, че всяка буква се замества само с една и съща друга буква, в целия текст.

Според някои исторически източници, този шифър е използван от [Гай Юлий Цезар](http://bg.wikipedia.org/wiki/%D0%AE%D0%BB%D0%B8%D0%B9_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80).

Математически запис:

За английската азбука използване mod=26, а за българската азбука mod =30.

Шифриране:

E_n(x) = (x + n) \mod {30}.

Дешифриране:

D_n(x) = (x - n) \mod {30}.

като n е ключа в случая n = 3, x е стойността на буквата.

**4. Използвани технологии**

Програмата е реализирано посредством Java език за програмиране в Eclipse IDE.

**5. Инсталация и настройки**

Необходимо е да имате инсталирана Java.

**6. Кратко ръководство на потребителя**

Стартираме програмата в Eclipse IDE. Тя предлага възможност на потребителя да избере да шифрира или да дешифрира текст съответно чрез въвеждане на буквата\символа „e“ за шифриране и на цифра „d“ за дешифриране. След направения избор, програмата изисква от потребителя да се въведе текст, а след това и какво е желаното от него отместване. При натискане на „Еnter” в конзолата се извежда резултата от извършеното по горе действие.

**7. Примерни данни**

При въвеждане на „e“ избираме да шифрираме. Въвеждаме „Hello“ с желано отместване „3“ резултата е „Khoor“.

При задаване на „d“ избираме да дешифрираме. Въвеждаме „Khoor“ с желано отместване „3“ резултата е „Hello“.

**8. Описание на програмния код**

При стартиране на програмата и въвеждане буквата\символа съответстваща на избора на потребителя source-кода извършва проверка посредством оператор *if*. Ако е въведено „*е*“ се изпълнява метод наречен „*encrypt”*, ако е въведено „*д*“ се изпълнява метод наречен „*decrypt“*, а ако е въведена друга буква\символ в конзолата се изписва „Wrong command !”. При изпълнението и на единия и на другия метод се изиска въвеждане на текст и отместване. Текста се превръща от променлива тип *String* в масив от *char* елементи (*char[]).*Чрез оператор *if* се прави проверка за стойността на отместването. С един *for* цикъл се обхожда масива, който пази в себе си буквите от азбуката и с още един - масива, който пази елементите на текста, който е въвел потребителя. Проверява се дали текущия елемент от масива който пази текста въведен от потребителя е еднакъв с елемент от масива в който се съдържат буквите от азбуката. След извършената по-горе проверка и в зависимост от това дали всички условия са изпълнени се извършва присвояването на елементите от въведения масив, +/- желаното отместване в нов масив. Чрез командата String.*valueOf*(); полученият *char* масив се превръща отново в променлива от тип *String*. Чрез команда *return* се извежда променливата от тип *String*, която пази шифрирания/дешифрирания текст.

**9. Приноси на курсиста, ограничения и възможности за бъдещо разширение**

Приложението е лесно и просто за употреба от потребителя.

**10. Използвани източници**

1.<http://bg.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%8A%D1%80_%D0%BD%D0%B0_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80>

2. „Въведение в програмирането с Java” – Светлин Наков и колектив, София 2008 г.