**Имена:** Владислав Катранкиев

**Дата: 31.01.2016 Предмет: Програмиране с Java, част 1**

**имейл:** vladovladivlado@abv.bg

**GitHub:** https://github.com/VKatrankiev/ProjectPlayFair

**Предаване:** Задачата се добавя към гитхъб repository, където е качен проекта

Шифроване чрез Плейфеър шифър

**1. Условие**

Въвежда се дума/изречение ключ и дума/изречение за шифроване. Използвайки правилата на Плейфеър, програмата връща шифрованата дума.

**2. Въведение**

Програмата е написана на компилаторът Eclipse.

**3. Теория**

Буквите от думата (изречението) ключ е вкарана в таблица 5х5 без те да се повтарят. Останалите букви от азбуката запълват остатъка от от таблицата по азбучен ред. Чрез правилата на Плейфеър програмата шифрира думата/изречението:

Ако думата за шифроване има повтарящи се букви, между тях се слага Х. Ако буквите са нечетен брой, накрая се слага Х (ако последната е Х, се слага Q)

Разглеждат се буквите по двойки. Ако са на един ред, се взимат последователно буквите от дясно. Аналогично ако са в колона – буквата отдолу. Ако не е нито един от случаите, се разглежда мислен квадрат и се взимат другите 2 върха. След размяната, се връща шифрованата дума.

**4. Използвани технологии**

Използван компилатор – Eclipse.

**5. Инсталация и настройки**

Програмата работи директно в платформата на Eclipse.

**6. Кратко ръководство на потребителя**

Въведете дума ключ в конзолата и дума за шифроване. Желателно е да няма други символи освен букви.

**7. Примерни данни**

Няма нужда от въвеждане на такива.

**8. Описание на програмния код**

Използвани са 3 класа :

TableGenerator, CipherMagic, PlayFairCipher. В първите два има по един метод. Съответно tableGenerator и convert. В последния е единствено main методът.

tableGenerator е метод, който връща матрица от символи. В него има проверка за некоректно зададени данни, която връща подходящо съобщение и null като return стойност. Входният аргумент на метода е от тип String. Буквите в променливата са превърнати в главни чрез метода .toUpperCase() на класа String. Променената входна променлива става аргумент на класа StringBuilder, от който са използвани методите .deleteCharAt(index) и .insert(index, <променлива от тип чар>) . Чрез тези методи се замества буквата J с буквата I, ако се намира в кодовата дума. Също така се премахват всички символи, които не са букви. Премахват се дублиращи букви от кодовата дума.

Въведен е обект от тип String alphabet. Той има стойност всички главни букви (без J) от английската азбука. От него се премахват буквите, които се съдържат в кодовата дума.

Започва манипулация отново над вече синтезираният String обект. Попълва се таблица от char елементи, като първо се слагат символите в получения String и после се добавят елементите от синтезираната азбука. Връща се получената таблица.

“convert” е метод, който за входни аргументи приема String и двумерен масив от символи.

Първоначално се прави проверка за коректно зададени данни и отново връща null при некоректни. Отново е използван методът .toUpperCase() над низа и след това стойността му е присвоена на обект от тип StringBuilder. Новият обект е пречистен от символи различни от главни латински букви. Проверява се дали низа съдържа J и се превръща в I. След което се добавя „Х“ между 2 еднакви букви, ако има такива. Ако има 2 „Х“, се добавя “Q” между тях. След това се проверява дали низът съдърва нечетен брой символи и се добавя “X” накрая, ако е така. Аналогично, ако последната буква е “X”, се добавя “Q”. След синтезирането на думата за шифроване започва проверяването на буквите по двойки. Намират се в таблицата и индексите им се запазват в променливи. След което, спрямо индексите, се определя по кое от правилата, описани в теорията ще се шифрират двойката букви. Така определените букви се записват последователно в едномерен масив от тип char. Инициализира се нов обект от тип StringBuilder, в който се присвояват всеки един от елементите на масива чрез методът .append(<променлива от тип char>). Чрез методът .toString обектът се връща като шифрирана дума (обект от тип String).

В main метода е инициализиран обект от тип Scanner, чрез който се чете от конзолата. В конзолата се принтират съобщения за улеснение на потребителя относно необходимата информация. На два обекта от тип String са присвоение необходимите данни за изпълнението на шифъра. В масив от тип char е присвоен резултата от изпълнението на метода tableGenerator от класа TableGenerator и след това е отпечатан в конзолата.

На екрана се принтира резултат от метода convert(<първи въведен обект>,<втори въведен обект>) от класа CipherMagic.

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

Програмата може да се използва за шифриране на съобщения при необходимост за секретно пренасяне на информация. Кодът може да се използва като основна логика за създаване на приложение, което шифрира съобщения.

**10. Използвани източници**

- http://stackoverflow.com/