**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, CipherLogic, PlayFairCipher (в PlayFairCipher се намира main метода). В класовете има множество методи. Главните са tableGenerator, и convert.

Преди да бъдат използвани обаче, (след проверка за коректност) данните от входа се преработват от методите synthesizeKeyword и synthesizeCipherWord, където се използва makeCipherable от основния клас, който привежда данните в удобен вид за правилно манипулиране от останалите класове.

tableGenerator е метод, който връща матрица от символи. Входният аргумент на метода е от тип String..

synthesizeKeyword и synthesizeCipherWord са методи на останалите два класа, но имат сходни функции. И двете правят съответните им променливи да могат да бъдат използвани от главните методи. Логиката обаче е различна при двата аргумента, зададени от конзолата.

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

След синтезирането на думата за шифроване започва проверяването на буквите по двойки от методът findLetters. Намират се в таблицата и индексите им се запазват в масив. След което, спрямо индексите, се определя по кое от правилата, описани в теорията ще се шифрират двойката букви. Това е изпълнено от метода playFairRules. Така определените букви се записват последователно в едномерен масив от тип char. Чрез методът String.valueOf(масива) 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. Чрез метода inputData се въвеждат 2та необходими аргумента за шифроване на думата. В него е използван метод isInputCorrect, който проверява коректността на въведеното. Понеже е методът е изпозлван и за двата входа, има проверка за това, кой от двата метода да ползва в зависимост дали е думата за шифроване или думата ключ.

**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/