**Имена:** Николай Георгиев

**Дата:** 27.01.18 **Предмет:** Програмиране с Java, част 1

**Имейл:** nikolaimgeorgiev@abv.bg  **GitHub:** <https://github.com/NikolaiMGeorgiev>

Шифроване чрез плейфеър шифър

**1. Условие**

Въвежда се дума ключ, която се поставя в таблица 5х5, така че да няма повтарящи се букви. След това таблицата се запълва с останалите букви от азбуката отново без повторения. Въвежда се и изречението, което трябва да се шифрова. На всяка двойка букви от него съответсва друга двойка, определена по следните правила, зависещи от разположението на изходната двойка букви в таблицата:

* Ако двете букви са на различни редове и различни колони, те образуват правоъгълник, на който те са двата срещуположни върха. Новата двойка се образува от буквите, които са другите два срещуположни върха.
* Ако буквите са на един ред, всяка буква от новата двойката съответства на буквата вдясно от входната. В частния случай, когато двойката се намира в края на реда и надясно няма повече букви, се избира първата буква (отляво) на долния ред.
* Подобно е и при двойка в една и съща колона. Разликата е, че се използва буквата под изходната, а когато няма такава (в най-долния ред на колоната), се преминава към най-горната буква на следващата колона.

Накрая се извежда полученото шифровано съобщение.

**2. Въведение**

Приложението е реализирано на платформата Java.

**3. Теория**

Алгоритъмът, работещ на Java, е реализирани с помощта на софтуера IntelliJ -интегрирана среда за разработка в Java за компютърен софтуер.

**4. Използвани технологии**

В програмата алгоритъмът първо проверява, дали въведените стойности са коректни (само английски букви). Следва запълване и принтиране в конзолата на таблицата. Принтира се и съобщението, разделено на двойки. Накрая чрез няколко метода се намират съответните шифровани двойки и се принтира получения текст.

**5. Инсталация и настройки**

Нужно е да имате инсталиран Java на компютъра си, който може да бъде изтеглен от <https://java.com/en/download/> , както и IntelliJ (<https://www.jetbrains.com/idea/download>). Програмата се отваря от PlayfairCipher в папка src.

**6. Кратко ръководство на потребителя**

Стартирайте програмата от Run>>Run ‘Playfair cipher’.

**7. Примерни данни**

Въведете думата ключ, например “playfair example”, след това натиснете “enter” и напишете желаното съобщение за кодиране като “Hide the gold in the tree stump”. След повторно натискане на “enter” ще се изведе шифъра.

**8. Описание на програмния код**

Използваните методи в програмата са:

* **correctEntry** - проверява коректността на входните данни
* **skippedLetter** - връща буквата, която ще бъде пропусната, за да се побере 26-буквената азбука в таблицата с 25 места
* **printTable** - принтира таблицата
* **insertX** - вмъква в съобщението буквата “X” там, където получената двойка букви се състои от еднакви букви или в случай, че съобщението е с нечетен брой букви, при което последната двойка се състои само от един елемент
* **encodeMessage** - построява и принтира крайния резултат и служи като връзка между getPositionInTable и getNewLetter
* **getPositionInTable** - връща на коя позиция в таблицата се намира дадената буква
* **getNewLetter** - връща съответната двойка шифровани букви; в нея се извикват sameColumnCase и sameRowCase, ако е нужно
* **getSameColumnLetters** / **getSameRowLetters** - връща съответната двойка букви в частните случаи, когато и двете букви са на един ред/колона

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

Програмата следва правилата на вече създаден шифър, поради което няма особени възможности за бъдещо развитие и е в завършения си вид. Като разширение може да се добави метод, който да разделя получения шифар на отделни думи.

**10. Използвани източници**

- <https://en.wikipedia.org/wiki/Playfair_cipher>