

Имена: Мирослав Шилов

Предмет: Програмиране с Java, част 1

Дата: 2017-01-19

имейл: stav\_ri@abv.bg

GitHub:<https://github.com/shilov1985/PlayfairCypherProgram>

# ПЛЕЙФЕЪР ШИФЪР

## 1. Условие

Програмата се стартира в средата за разработка Еклипс.

1. Въвежда се текста за шифроване
2. Въвежда се думата-ключ
3. Извежда се шифрвания текст

## 2. Въведение

Приложението е реализирано на платформата Java и се стартира в средата за разработка Еклипс. Представлява програма, която шифрова текст, чрез Плейфеър шифър.

## 3. Теория

Програмата шифрова текст, който се въвежда от потребителя. Това е конзолно приложение, тоест няма графичен интерфейс.

## 4. Използвани технологии

В текущата програма алгоритъмът най-напред проверява дали сме въвели текст за шифроване, и ако не сме се извежда съобщение за грешка. Програмата също така филтрира входа, така че приема за обаработка само тези символи от текста, отговарящи на главните и малки букви от английската азбука.

## 5. Инсталация и настройки

Трябва да имате инсталирана Java на компютъра си, която може да изтеглите от тук: <https://java.com/en/download/>, след което добавяте проекта на програмата в Еклипс.

Проекта може да намерите тук: <https://github.com/shilov1985/PlayfairCypherProgram>.

След като сте добавили проекта в Еклипс стартирайте java файла: RunProgram.java, намиращ се отляво в експлорера на пакети.

## 6. Кратко ръководство на потребителя

Стартирайте програмата. В конзолата ще се изведе информация за това какво тя прави. Въведете текста за шифроване и натиснете Enter. След това

програмата ви подканя да въведете ключ за шифроване и да натиснете Enter. Ако не въведете ключ, програмата ще запълни матрицата със символите от английската азбука, без "J".

Като резултат се извежда матрицата и шифрваният текст.

## 7. Примерни данни

Въвеждаме текст за шифроване, например "Hide the gold in the tree stump" .

Въвеждаме ключ за шифроване, например "playfair example" .

Матрицата се запълва по следния начин:

P	L	A	Y	F <sup>A</sup>
I	R	E	X <sup>A</sup>	M <sup>PLE A</sup>
B	C	D <sup>EF</sup>	G	H <sup>I=J</sup>
K <sup>LM</sup>	N	O <sup>P</sup>	Q <sup>R</sup>	S
T	U	V	W <sup>XY</sup>	Z

Като резултат имаме шифрован текст :BMODZBXDNABEKUDMUIXMMOUIVF

## 8. Описание на програмния код

Програмата се състои от четири джава файла.

CipherKey.java-Съдържа клас с име CipherKey и метод fixKeyForCoding, отговарящ за форматирането на ключа, с които шифроваме текст.

Например ако имаме ключ: playfair example, методът премахва повтарящите се букви, като ако имаме буква 'J' я замества с 'I'.

Резултатът е: PLAYFIREXM

RestLettersForMatrix.java-Съдържа клас с име RestLettersForMatrix и метод getRestLettersForMatrix , отговарящ за инициализацията на масив със символите от английската азбука без 'J' , които не присъстват в ключа.

SentenceForCoding.java-Съдържа клас с име SentenceForCoding и метод convertSentens , отговарящ за форматирането на текста, който искаме да шифроваме.

Например ако текста, който ще шифроваме е "Hide the gold in the tree stump" разделяме го на двойки букви. Преди това обаче добавяме X ако има еднакви букви една до друга.

Резултата е:

HIDETHEGOLDINTHETREXESTUMP

Има и някои особености които трябва да се имат в предвид.

Ако в текста за шифроване имаме да разделяме буквите 'XX' правим това с буквата 'Q',но във всички други случай разделяме с 'X'.Също ако имаме нечетна дължина на текста и ако имаме за последна буква 'Q' добавяме на края 'X',но ако имаме 'X' добавяме 'Q';

Примери:

'XX' се преобразува в 'XQXQ'

'QQ' се преобразува в 'QXQX'

'AA' се преобразува в 'AXAX'

'AAQ' се преобразува в 'AXAQ'

RunProgram.java-В този клас комбинираме всички методи за да може програмата да работи.Тук са и алгоритмите за извличане на шифрованите букви по редове, колони и квадрати(правоъгълници),като е изпълнено и условието :ако буквите са последни от дадена колона, взимаме първата буква на следващата колона. Същото за ред.

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

Програмата е лесна за работа,а условието,ако буквите са последни от дадена колона да взимаме първата буква на следващата колона,което важи и за редовете,я прави различна и оригинална.Може да се направи дешифрираща програма ,която да преобразува шифрваният текст в почти първоначалния му вид.

Също така,може да се добавят опции,като например потребителя да избира в каква посока да се вземат шифрованите букви,или коя с каква буква да се замести.

## 10. Използвани източници

[https://en.wikipedia.org/wiki/Playfair\\_cipher](https://en.wikipedia.org/wiki/Playfair_cipher)

<http://rumkin.com/tools/cipher/playfair.php>