Име: **Емил Сергиев**
е-поща: emilsergiev@abv.bg
уеб сайт: http://emil.free.bg

Дата: 28/01/2017
Курс: Програмиране с Джава - 1
GitHub: https://github.com/emilsergiev

Разбиване на Цезар шифър

1. Условие

При въведен Цезаров шифрован текст да се изведе дешифрования, без да се знае ключът (номера на отместване).

- Знае се, че най-често срещаните букви в английския са e, t, h
- Намира се най-често срещания символ във въведения текст
- Пресмята се колко е от-местването от него до e, t, h (ако най-често срещания символ е една от тези букви, тогава използваме буквата “a”)
- Извеждат се трите варианта за първо-начален текст
- Ако потребителя не е доволен се извеждат и останалите 22 варианта на текста

По-добър вариант:

- Думите за всеки от 25-те варианта на текста се сравняват с въведен английски речник от 10000 най-често срещани думи.
- Текста при който има най-много думи, които са от речника, се извежда на екрана

Най-добър вариант:

★ **Проекта да използва метод с речник и да включва графичен интерфейс!**

2. Въведение

Нашето приложение е реализирано на платформата Джава.

3. Теория

Визуалните елементи, както и самият алгоритъм работещ под Джава са реализирани с помощта на софтуера Eclipse - многоезична среда за разработка на софтуер, която включва интегрирана среда за разработка (IDE) и плагин система.

4. Използвани технологии

За графичен интерфейс използвах плагинът Window Builder на софтуера Eclipse. За звуковия файл използвах морз код звуков генератор и превърнах в .au формат. А за Windows изпълнимия .exe файл (който е обвивката на изпълнимия .jar файл) използвах софтуера launch4j.

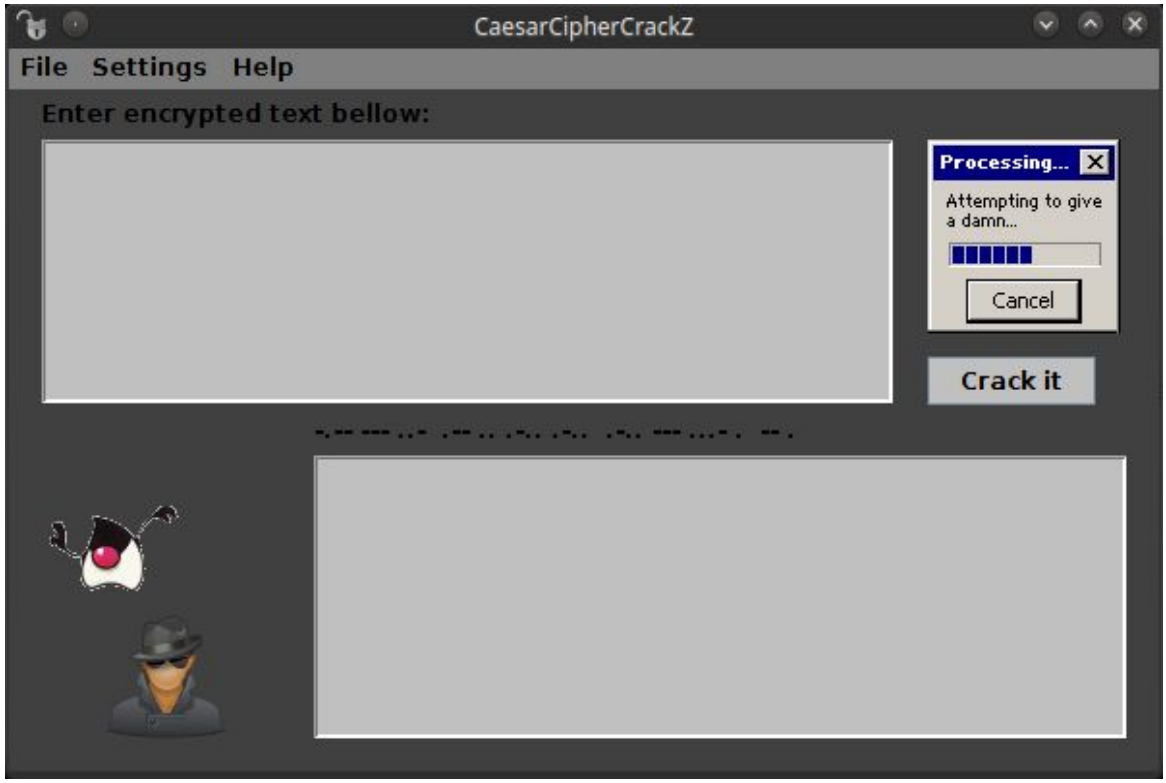
5. Инсталация и настройки

Windows: За да стартираме графичния интерфейс не е нужно да имаме инсталирана Джава на компютъра си! Просто щракваме и стартираме Caesar.exe файла. Ако в системата нямаме инсталирана Джава тогава софтуера сам ще я изтегли от java.com и ще я инсталира. Ако това не проработи по някаква причина тогава ще имаме опцията сами да го направим след като нашето приложение ни отведе на https://java.com/en/download/ сайта.

Linux и Mac: Трябва да имаме инсталирана Джава на компютъра си! Може да я инсталираме от тук: https://java.com/en/download/. Стартираме нашата конзола за команди и от там отиваме до папката където се намира Caesar.jar файла. За Linux, написваме следната команда в конзолата: **java -jar Caesar.jar** а за Mac, написваме: **java -cp Caesar.jar menu.Menu**

6. Кратко ръководство на потребителя

При стартиране на програмата ще бъдем посрещнати от следния прозорец:

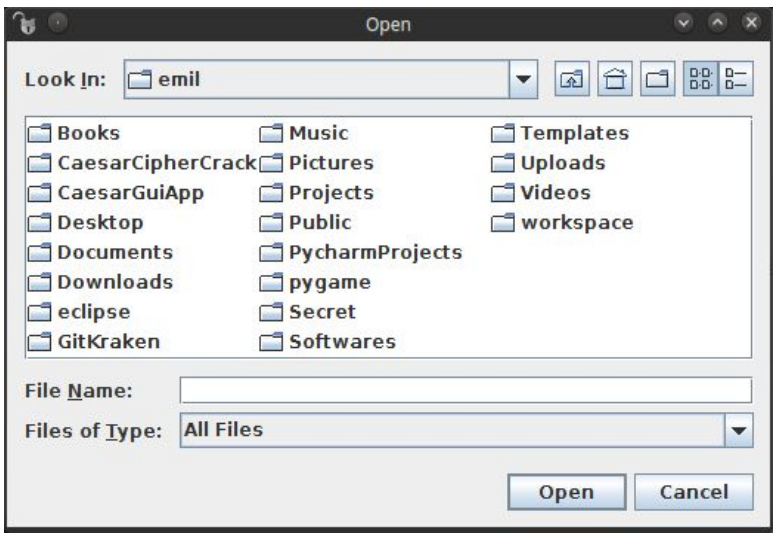


Това е как изглежда на моята операционна система **Linux!**
Джава кода е написан така, че да има “LookAndFeel” на съответната операционна система…
Затова, под Windows или Mac ще има “по-грозен” интерфейс :p ;-)

От горната меню-лента, можем да изберем три опции: **File**, **Settings** или **Help**.

Под **File** падащото се меню можем да изберем три опции: **Open**, **Save**, или **Exit**.

- **Open** - отваря файл и текста от него се показва в областта на въвеждане за текст.



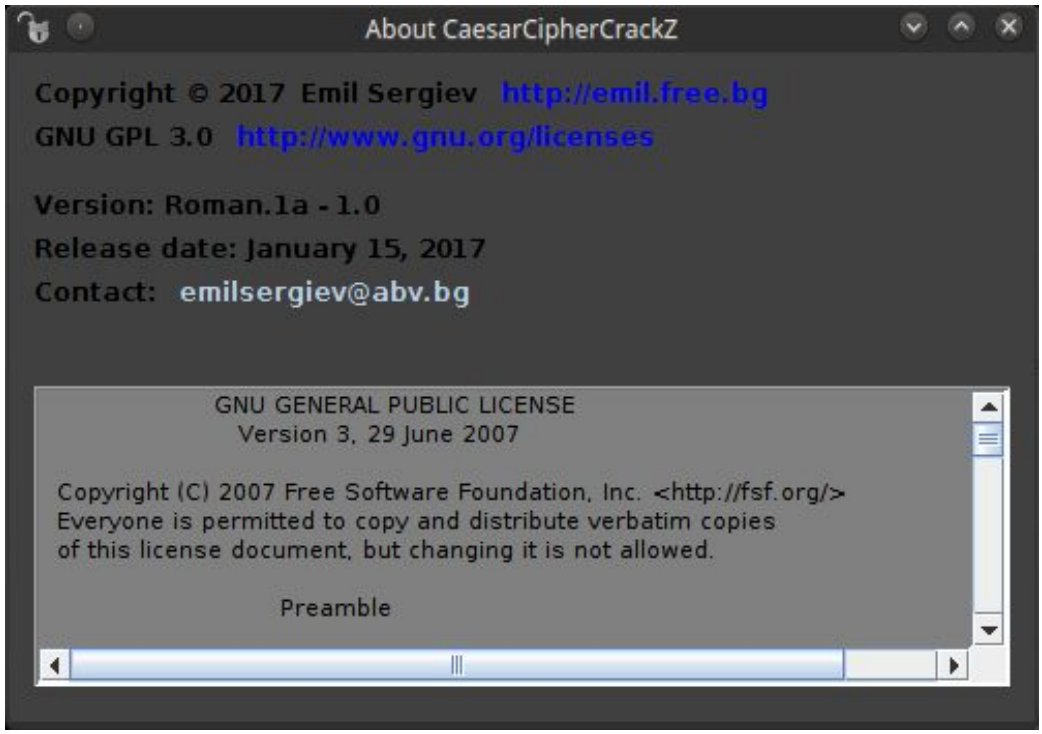
- **Save** - записва текста от областта на изходния текст във файл на място където ние посочим (интерфейса е същия като при Open).
- **Exit** - излиза от софтуера и прекратява програмата.

Под **Settings** падащото се меню можем да изберем една от двете “радио-бутонни” опции:

- **English dictionary** - която е избрана по под-разбиране и използва 10000 най-често срещаните английски думи за разбиване на кода.
- **Brute force attack** - е другата опция, която може да изберем за да получим всичките 25 ключови версии на шифрования текст или да си шифроваме наш собствен текст.

Под **Help** падащото се меню в момента има само една опция:

- **About** - отваря нов прозорец и показва информация за версията на софтуера, дата на издаване, електронна поща за контакти и GNU GPL 3.0 лицензa който се чете от файл.



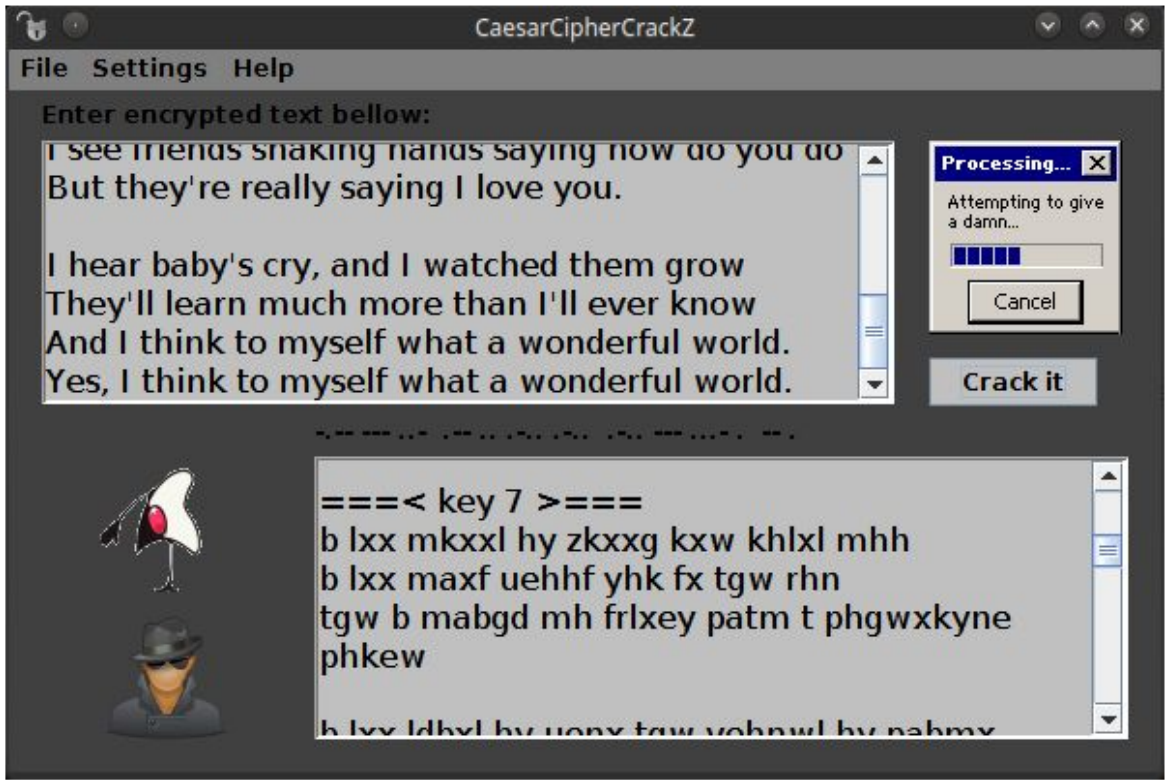
Сините връзки може да се щракат и да ни изпратят на съответните уеб-сайтове… Но, връзката на електронна поща emilsergiev@abv.bg съм я деактивирал за сега защото чупи (замразява) софтуера ако нямаме инсталирана електронно-пощенско приложение на компютъра си и щракнем на нея... затова е и с по различен цвят.

* В бъдещи версии на софтуера може да прибавим подобно на това “кратко ръководство на потребителя” като още една опция под **Help** падащото се меню… Но, нашето приложение е толкова просто и лесно за употреба, че не виждам смисъл да го правим в момента.

Питате как може да шифроваме собствен текст?

1. Може да пишем обикновен текст в областта за въвеждане на текст или направо да отворим текстов файл от **File** и **Open** менюто.

2. Избираме **Brute force attack** от падащото се меню на **Settings** и щракваме върху бутона **Crack it**.



- В областта на дисплея ще се покаже всичките 25 ключови криптирани версии на нашия текст. Копираме и поставяме версията която ни харесва в съобщението до нашия получател... Или използваме опцията **Save** от **File** падащото се меню за да запишем всичките шифровани версии във файл за използване на по-късен етап...

7. Примерни данни

1. Пишем следния примерен текст в областта за въвеждане на шифрован текст:

   b lxx mkxxl hy zkxxg kxw khlxl mhh
   b lxx maxf uehhf yhk fx tgw rhn
   tgw b mabgd mh frlxey patm t phgwxkyne phkew

   b lxx ldbxl hy uenx tgw vehnwl hy pabmx
   max ukbzam uexllxw wtr max wtkd ltvkxw gbzam
   tgw b mabgd mh frlxey patm t phgwxkyne phkew

   max vhehkl hy max ktbguhp lh ikxmmr bg max ldr
   tkx telh hg max ytvxl hy ixhiex zhbgz ur
   b lxx ykbxgwl latdbgz atgwl ltrbgz ahp wh rhn wh
   unm maxrkx kxteer ltrbgz b ehox rhn

   b axtk uturl vkr tgw b ptmvaxw maxf zkhp
   maxree extkg fnva fhkx matg bee xoxk dghp
   tgw b mabgd mh frlxey patm t phgwxkyne phkew
   rxl b mabgd mh frlxey patm t phgwxkyne phkew

2. Натискаме бутона **Crack it**.
3. Получаваме следния дешифрован текст:

i see trees of green red roses too
i see them bloom for me and you
and i think to myself what a wonderful world

i see skies of blue and clouds of white
the bright blessed day the dark sacred night
and i think to myself what a wonderful world

the colors of the rainbow so pretty in the sky
are also on the faces of people going by
i see friends shaking hands saying how do you do
but theyre really saying i love you

i hear babys cry and i watched them grow
theyll learn much more than ill ever know
and i think to myself what a wonderful world
yes i think to myself what a wonderful world

Просто и лесно е като “1, 2, 3” дори само 1, 2 и готово ^.^

Както забелязваме нашето приложение преобразува всички главни букви в малки. Също така изчиства всички апострофи, точки, запетайки и т.н. Но, това може лесно да се промени в бъдещите версии ако решим, че е по-добре да ги използваме.

8. Описание на програмния код

Метода **main**: Стартира нашето приложение, наглася “LookAndFeel” на съответната операционна система, създава рамката и я прави видима.

- ➔ UIManager.setLookAndFeel(UIManager.getSystemLookAndFeelClassName());
- ➔ CaesarGui frame = new CaesarGui();
- ➔ frame.setVisible(true);

После **CaesarGui()** извиква методите **initSound**, **initComponents**, и **createEvents**.
Метода **initSound**: Инициализира звука с файла “*secretcode.au*” (това е нашето тайно послание с под-съзнателна команда за да програмира мозъка на потребителя) в цикъл.
Метода **initComponents**: Съдържа всичкия код за създаване и инициализиране на компоненти (надписи, областите за въвеждане/извеждане на текст, менюта, бутони, иконки и т.н.)
Метода **createEvents**: Съдържа всичкия код за създаване на събития.
Метода **readDictionary**: Връща масив от 10000 най-често срещани английски думи.
Метода **allSolutions**: Връща масив с всичките 25 варианта на де/шифроване.
Метода **decrypt**: Връща символна нишка на даден вариант от де/шифроването.
Метода **findBestMatch**: Връща байт на ключа за най-подходящия вариант според речника.

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

Нашето приложение е просто и лесно за употреба. Може да има полза за влюбените тинейджъри за да си разменят тайни послания без родителите им да знаят какво си пишат... Или за възрастните да разбиват тайната кореспонденция на техните деца и тинейджъри… Това приложение няма възрастова граница за потребители. В бъдещи версии на това приложение може да се добавят още много други функции и/или да се интегрира в “email client”.

10. Използвани източници

Java Gui Design w/ WindowBuilder Designer (part 1, 2, 3, 4, 5)
https://www.youtube.com/watch?v=KdTsY3G_To0