

Paralelní programování

Robert Čížek, Lukáš Hlavatý, Peter Smatana

25. června 2017

Zadání projektu

Cílem projektu bylo vytvořit program který se snaží hrubou silou rozšifrovat šifrový text. Šifrový text je vytvořený pomocí Vigenèrovy šifry.

Požadavky na softwarové vybavení Projekt je vytvořený v programovacím jazyku Java ve verzi 1.7. Pro vytvoření struktury projektu, pro běh a tvorbu *.jar* souborů používáme technologii Maven. Pro běh projektu je třeba mít nainstalované Java Runtime Environment. Pro práci na projektu je třeba mít Java Development Kit.

Popis projektu

Naše řešení je schopno text šifrovat i dešifrovat. Šifrování se provádí ve třídě **Encryptor** v metodě **Encrypt**. V této metodě iterujeme nad otevřeným textem a podle klíče jej šifrujeme. O to se stará třída **Alphabet**, která má metody **shiftUp** a **shiftDown**. Metoda **shiftUp** šifruje text podle klíče a metoda **shiftDown** dešifruje text podle klíče. Ve skutečnosti se jedná o hledání patřičného znaku ve Vigenèrově čtverci.

Ve zdrojovém kódu č. 1 je vidět jak se pracuje Vigenèrovým čtvercem. Nalezení zasifrovaného znaku je přičtení ordinální pozice znaku klíče v ASCII tabulce.

```
1 public static char shiftUp(char c, char key) {
2     int num = (int) c - 97;
3     if ((num >= 0) && (num <= 25)) {
4         num += (int) key - 97;
5         if (num > 25) {
6             num -= 26;
7         }
8         return alphabet.charAt(num);
9     } else {
10        return c;
11    }
12 }
```

Zdrojový kód č. 1: Šifrování znaku podle znaku v klíči.

Pro dešifrování máme třídu **Decryptor** ve které jsou tři metody kde uplatňujeme odlišné přístupy na dešifrování. První metoda **KeyDecrypt** dešifruje text inverzně stejně jako je implementováno šifrování. Vezme šifrový text, klíč a obdobně jako v ukázce zdrojového kódu č. 1 dešifruje text. Druhý přístup reprezentuje metoda **FreqDecrypt**, která provádá frekvenční analýzu. Frekvenční analýza je přístup, jak najít v šifrovém textu nějakou podobnost s přirozeným jazykem, ve kterém je zpráva napsaná. Poslední přístup je hledání klíče hrubou silou podle slovníku. Hádáme klíč, klíčem rozšifrováváme slovo a toto slovo hledáme ve slovníku.

Paralelní vylepšení programu

asd asd asd

Měření

takhle se dělají v L^AT_EXu tabulky:

1	xy	3
4	5	6
7	8	9

Závěr

asd asd asd