Prof. Dr. Harald Brandenburg
Hochschule für Technik und Wirtschaft (HTW)
Fachbereich 4 (Wirtschaftswissenschaften II)
Wilhelminenhofstraße 75 A
12459 Berlin (Oberschöneweide)
Raum WH C 605

Fon: (030) 50 19 - 23 17
Fax: (030) 50 19 - 26 71
h.brandenburg@htw-berlin.de

Dienstag, 17. Juni 2014

Programmierung 2

SS 2014

Aufgabe 12: **Gruppe 1:** 15.07.2014 **Gruppe 2:** 08.07.2014

Schreiben und dokumentieren Sie ein Programm, mit dem Textdateien mit der unten beschriebenen Variante des Vigenère-Verfahrens verschlüsselt werden können.

- Dem Programm sollen beim Aufruf genau vier Argumente übergeben werden. Kommt es dabei zu einem Fehler, soll auf dem Bildschirm ein Hinweis zur Bedienung des Programms erscheinen, dem insbesondere entnommen werden kann, welche Parameter in welcher Reihenfolge anzugeben sind:

```
Benutzung:  java ProgrammName <option> <schluesselwort> <quelldatei> <zieldatei>
wobei:
  option            -v          verschluesseln
  option            -e          entschluesseln
  schluesselwort    Buchstaben, Ziffern und viele andere Zeichen enthalten darf
  quelldatei        eine Textdatei sein muss, die geoeffnet werden kann
```

- Das Schlüsselwort soll nicht nur Buchstaben (klein oder groß) und Ziffern enthalten dürfen, sondern auch (möglichst viele) andere Zeichen.[1] Ob es zulässig ist, soll mit Hilfe eines regulären Ausdrucks festgestellt werden.

- Es ist bereits beim Aufruf des Programms zu überprüfen, ob die Quelldatei geöffnet werden kann.

- Wenn alles in Ordnung ist, soll das Programm den in der Quelldatei enthaltenen Text lesen, mit dem Schlüsselwort ver- oder entschlüsseln und den ver- oder entschlüsselten Text in der Zieldatei speichern:

```
Ich verschluessele die Datei  MeineDatei.java  mit dem Schluesselwort  co=De#.-08+15  .
Fertig.
```

- Die Quelldatei soll dabei unverändert erhalten bleiben.

- Wenn es die Zieldatei bereits gibt, soll das Programm auf Wunsch abgebrochen werden können:

```
Ich verschluessele die Datei  MeineDatei.java  mit dem Schluesselwort  co=De#.-08+15  .
Achtung: Datei test.txt ist schon vorhanden!
   Ueberschreiben (j/n) ?  j
Fertig.
```

1 Dabei ist aber darauf zu achten, dass es nicht zu Konflikten mit dem Kommandointerpreter der Shell kommt (**bash**).

Zum Verschlüsseln der Texte soll (der Einfachheit halber) das klassische Vigenère-Verfahren wie folgt benutzt werden.[2] Dessen Grundidee ist einfach zu verstehen:

```
Dies ist – zum Beispiel – der zu verschluesselnde Text.
```

Und dies ist das Schlüsselwort: `Osterhase`
Das Schlüsselwort wird dem Text (gedanklich) fortlaufend so unterlegt:

```
Dies ist – zum Beispiel – der zu verschluesselnde Text.
Oste rha – seO sterhase – Ost er haseOsterhaseOst erha.
```

Benötigt wird jetzt noch eine Funktion `v`, die je zwei Buchstaben `x` und `y` genau einen Buchstaben `v(x,y)` zuordnet. Im Beispiel besteht der verschlüsselte Text dann aus den Buchstaben

`v(D,O), v(i,s), v(e,t), v(s,e), ... v(T,e), v(e,r), v(x,h), v(t,a)`

Damit der Text nach dem gleichen Verfahren wieder entschlüsselt werden kann, muss `v` allerdings so gewählt werden, dass es eine Umkehrfunktion `e` gibt, die je zwei Buchstaben `z` und `y` genau einen Buchstaben `x = e(z, y)` so zuordnet, dass für alle Buchstaben `x` und `y` stets

`e(v(x,y),y) = x`

ist. Blaise de Vigenère hat vorgeschlagen, `v` und `e` einfach wie folgt als Verschiebungen zu realisieren.

Man stelle sich vor, dass die großen und kleinen Buchstaben des Alphabets auf einem biegsamen Band aufgereiht sind.[3] Unwesentlich ist es, in welcher Reihenfolge. Sie können (und sollten!) beliebig gemischt sein. Für jeden Buchstaben `x` sei `Pos(x)` die Position, an der er in der Aufreihung vorkommt.

Man definiere nun `v` so, dass `v(x,y)` der Buchstabe ist, der an der Stelle `Pos(x) + Pos(y)` steht, d.h. der durch Verschieben von `x` um `Pos(y)` Stellen nach rechts erhalten wird. Dabei kann es allerdings vorkommen, dass `Pos(x) + Pos(y)` eine Stelle ergibt, die hinter der letzten Stelle des Bandes liegt. In diesem Fall stelle man sich vor, dass das Band zu einem Kreis gebogen ist, so dass es nach der letzten Stelle wieder vorne weitergeht.

Die Umkehrfunktion `e` definiere man analog durch entsprechendes Verschieben nach links.

- Ihr Programm soll aber nicht nur Buchstaben verschlüsseln, sondern auch möglichst viele andere Zeichen, insbesondere alle, die in C- oder Java-Progammen vorkommen können (d.h. auch Tabulatoren, Leerzeichen und `\n`, wodurch sich die Zeilenstruktur des Textes ändert).

- Es ist bekannt, dass ein nach dem Vigenère-Verfahren verschlüsselter Text für Angreifer besonders schwer zu entschlüsseln ist, wenn das Schlüsselwort mindestens so lang ist wie der zu verschlüsselnde Text.[4] Ihr Programm soll daher das übergebene Schlüsselwort zunächst durch ein von Ihnen zu erfindendes, möglichst undurchsichtiges Verfahren auf die Länge des zu verschlüsselnden Textes verlängern und den Text dann tatsächlich mit dem verlängerten

2 Es wurde vom französischen Diplomaten Blaise de Vigenère (1523 – 1596) erfunden und galt bis Mitte des 19.Jahrhunderts als sicher.
3 Analog zu den Zahlen auf einem Zentimetermaß.
4 Siehe z.B. http://de.wikipedia.org/wiki/Vigenère-Chiffre

Schlüsselwort verschlüsseln.[5]

[**Hinweise:**

- Bei der Präsentation Ihrer Lösung sollen Sie (eine der) Dateien Ihres Programms verschlüsseln, anschließend entschlüsseln und das Programm dann erneut übersetzen.

]

5 Die Verlängerung des Schlüsselwortes muss natürlich für das Entschlüsseln reproduzierbar sein.