Übung

Datenvisualisierung und GPU-Computing

Dozent: Michael Vetter
michael.vetter@rrz.uni-hamburg.de

Sommersemester 2013

Aufgabe 1: *Vingenère Verschlüsselung*

Mit einem Vingenère-Schlüssel (auch Verschiebe-Schlüssel genannt) kan man Texte verschlüsseln. Man benötigt dazu ein Passwort und das Vingenère-Quadrat:

	abcdefghijklmnopqrstuvwxyz
A	ABCDEFGHIJKLMNOPQRSTUVWXYZ
B	BCDEFGHIJKLMNOPQRSTUVWXYZA
C	CDEFGHIJKLMNOPQRSTUVWXYZAB
.	.
.	.
.	.
Y	YZABCDEFGHIJKLMNOPQRSTUVWX
Z	ZABCDEFGHIJKLMNOPQRSTUVWXY

Zur Verschlüsselung legt man das Passwort über den Klartext und verschlüsselt dann buchstabenweise, indem man den verschlüsselten Buchstaben dem Vingenère-Quadrat entnimmt. Die Spalte ist dabei durch den Klartextbuchstaben, die Zeile durch den Passwortbuchstaben gegeben.

Ein Beispiel:

Klartext:	datenvisualisierung und gpu computing
Passwort:	HAMBURGHAMBURGHAMBU RGH AMB URGHAMBUR
Verschlüsselt	KAFFHMOZUMMCJOLRGOA LTK GBV WFSWUFJHX

Der Einfachheit halber soll der Text nur aus Kleinbuchstaben (keine Umlaute, keine Satzzeichen, keine Zahlen, etc.) und Leerzeichen bestehen. Leerzeichen werden nicht verschlüsselt. Das Passwort besteht nur aus Großbuchstaben ohne Leerzeichen.

Der zu ver-, bzw. entschlüsselnde Inhalt soll aus einer Datei gelesen werden. Dabei hat diese die oben genannten Anforderungen an den Klartext zu erfüllen.

Schreiben Sie ein Programm, mit folgenden Funktionen:

1. Warten auf Benutzereingabe: 'v', 'e', 'q'.
2. Beende das Programm bei 'q'.
3. Frage Dateinamen ab bei 'v' und 'e'.
4. Lese die Datei ein und gebe diese auf dem Bildschirm aus.
5. Entschlüssel den Dateiinhalt bei 'e' und gebe in am Bildschirm aus.
6. Verschlüssel den Dateiinhalt bei 'v' und gebe in am Bildschirm und in eine Datei aus.
7. Beginne bei 1.

Hinweis: Die Größe einer Datei können Sie bei Nutzung von File-Streams mittels der Methoden *seekg()* und *tellg()* abfragen. Das byteweise Einlesen von Dateien kann über die Methode *get()* realisiert werden.