

## Übung 1

Abgabetermin: 20. Oktober 2011 **vor** der Vorlesung

**Wichtig:** Bitte lesen Sie die allgemeinen Hinweise zu den Übungsaufgaben, welche sich in dem Hauptverzeichnis „Übungen“ im Blackboard befinden.

### 1. Angriff auf eine Substitutionschiffre

Im Übungsverzeichnis befindet sich ein verschlüsselter Text in der Datei „chifftrat.txt“, der mit der Substitutionschiffre verschlüsselt wurde. Ziel dieser Aufgabe ist es, den Klartext wiederzugewinnen, d.h. das Chifftrat zu entschlüsseln. Gehen Sie dabei wie folgt vor:

- (a) Geben Sie die relative Häufigkeit der Buchstaben A bis Z des Chiffrates an. (10 Pkt.)
- (b) Entschlüsseln Sie einen Absatz aus der Datei „chifftrat.txt“ im Übungsverzeichnis mit Hilfe der folgenden Häufigkeitsverteilung (Prozentangaben) der enddeutschen Sprache. Da der Text recht kurz ist, kann die allgemeine Häufigkeitsverteilung nicht 100% übernommen werden. Umlaute sind als in der Form UE, AE und OE dargestellt, ß ist ein eigener Buchstabe. Die Häufigkeitsverteilungen für andere Sprachen finden sie z.B. bei Wikipedia: <http://de.wikipedia.org/wiki/Buchstabenhäufigkeit> (25 Pkt.)

Buchstabe	Häufigkeit	Buchstabe	Häufigkeit	Buchstabe	Häufigkeit
A	6.51	J	0.27	S	7.27
B	1.89	K	1.21	T	6.15
C	3.06	L	3.44	U	4.35
D	5.08	M	2.53	V	0.67
E	17.40	N	9.78	W	1.89
F	1.66	O	2.51	X	0.03
G	3.01	P	0.79	Y	0.04
H	4.76	Q	0.02	Z	1.13
I	7.55	R	7.00	ß	0.31

- (c) Geben Sie die verwendete Substitutionstabelle an. (5 Pkt.)
- (d) Aus welchem Buch stammt der Text ? Wie heißt der Autor ?  
(Wenn nötig recherchieren Sie im Internet.) (5 Pkt.)

### Hinweise:

- Sie dürfen den Text auch elektronisch bearbeiten (beispielsweise, indem Sie ein Programm zur Ermittlung der Buchstabenhäufigkeit erstellen). .
- Die Entschlüsselung ist auch per Hand möglich. Es empfiehlt sich hierbei, Kleinbuchstaben für den Klartext und Großbuchstaben für das Chifftrat zu verwenden.
- Die Suchen/Ersetzen Funktion in Ihrem Texteditor könnte nützlich sein.