



## 2. Übung zur Vorlesung „Datensicherheit“

Sommersemester 2005

18. April 2005

Abgabe: 02.05.2004 in der Übung

### Aufgabe 2.1:

(6 Punkte)

Folgender chiffrierter Text wurde mit Hilfe eines einfachen Substitutionsalgorithmus erstellt:

53†††305))6\*;4826)4†.)4†);806\*;48†8π60))85;1†(:;†\*8†83(88)  
 5\*†;46(;88\*96\*?;8)\*†(;485);5\*†2:\*†(;4956\*2(5\*-4)8π8\*;40692  
 85);)6†8)4††;1(†9;48081;8:8†1;48†85;4)485†528806\*81(†9;48;(88;  
 4(†?34;48)4†;161;:188;†?;

Entschlüsseln Sie den Text unter Benutzung folgender Hinweise:

- Der im Englischen am häufigsten vorkommende Buchstabe ist 'e'. Das am häufigsten oder zweithäufigsten auftretende Zeichen steht also möglicherweise für das 'e'. Es tritt häufig auch paarweise auf, z.B. in 'meet', 'street', 'been', 'agree' usw. Versuchen Sie, ein Zeichen im Text zu finden, das mit 'e' entschlüsselt wird.
- Das im Englischen am häufigsten auftretende Wort ist 'the'. Nutzen Sie diese Tatsache, um die Zeichen für 't' und 'h' zu erraten.
- Entschlüsseln Sie den Rest der Nachricht, indem Sie weitere Worte ableiten.

Die sich ergebene Nachricht ist zwar englischer Text, ergibt aber beim ersten Durchlesen unter Umständen wenig Sinn.

### Aufgabe 2.2:

(5 Punkte)

Schreiben Sie ein Programm, das eine Textanalyse durchführt. Hierbei soll von einem gegebenen Text die Häufigkeit der vorkommenden Buchstaben berechnet werden. Der Unterschied von Groß- und Kleinschreibung sowie Satz- und Sonderzeichen sollen ignoriert werden.

In einer Variante des Programms berücksichtigen Sie den Wortabstand, Sonderzeichen, wie !,?, usw. als ein Zeichen \*.

Analysieren Sie mit Ihrem Programm die beiden Texte *lit.txt* und *gnu.txt*, die als Text-Files auf der Homepage zu finden sind. Bestimmen Sie die Entropie der Texte.

### Aufgabe 2.3:

(3 Punkte)

Modifizieren Sie die BEZOUT-Gleichung aus dem erweiterten EUKLIDischen Algorithmus aus der Aufgabe 9 zum Invertieren primen Restklassen.

- Bestimmen Sie  $\text{ggT}(1234567893987654321, 311111111111111112)$ .
- Geben Sie alle ganzzahligen Lösungen von  $1234567893987654321x + 311111111111111112y = 3$  an.
- Berechnen Sie  $311111111111111113^{-1} \bmod 1234567893987654321$ .