



1. Übung zur Vorlesung „Datensicherheit“

Sommersemester 2005

1. April 2005

Abgabe: 18.04.2004 in der Übung

Aufgabe 1.1:

(3 Punkte)

Schreiben Sie ein Programm, daß für ein gegebenes $g \in \mathbb{N}, g > 1$, die g -adische Darstellung einer natürlichen Zahl n berechnet. Berücksichtigen Sie insbesondere das Hexadezimalsystem ($g = 16$).

Aufgabe 1.2:

(2+2 Punkte)

Das Alphabet $\{A, B, C, \dots, X, Y, Z\}$ wird nach CAESAR codiert. Schreiben Sie ein Programm, das einen eingegebenen Text verschlüsselt.

Verwenden Sie das Programm, um folgenden Text

```
PME SDGZPXQSQZPQ BDANXQY PQD
WAYYGZUWMFU AZ NQEFQTF PMDUZ QUZQ
ZMOTDUOTF IUQPQDLGSQNQZ, PUQ MZ
MZPQDQD EFQXXQ SQEQZPQF IGDPQ.
```

zu entschlüsseln. Probieren Sie hierzu alle möglichen Schlüssel, und identifizieren Sie den dechiffrierten Text. (Den Text finden Sie als ASCII-File auf der Homepage.)

Aufgabe 1.3:

(4 Punkte)

Berechnen Sie mit Hilfe eines Programmes für zwei gegebene ganze Zahlen m, n den größten gemeinsamen Teiler $\text{ggT}(m, n)$. Benutzen Sie hierzu den in der Übung vom 11. 04. 2005 vorgestellten EUKLIDischen Algorithmus.

Benutzen Sie eine Möglichkeit zur Rechnung mit großen Zahlen.