Übungsaufgaben zur Vorlesung **Diskrete Mathematik für Informatiker**, WS 2010/2011

Blatt 7

Hinweis: Sie brauchen nichts abzutippen. Die Zahlen und Funktionsdefinitionen in Aufgabe 28 finden sie unter http://mfi.math.uni-siegen.de/dmi/dmi-uebg-07.txt

27. Im RSA-Algorithmus sei $p = 17$, $q = 23$, $n = pq$ und $e = 31$.
(a) Verschlüsseln Sie die Zahl 101 mit dem öffentlichen Schlüssel (e, n).
(b) Bestimmen Sie den geheimen Schlüssel (d, n) und entschlüsseln Sie Ihr Ergebnis.

28. Im RSA-Algorithmus sei

```
p = 3235021270138411515388415126349303161830478757812712222746662306007099611832629424005861721636586215841849797940736 3

q = 2682897143690027153759156209250397022629408304195712960455258413499718879302722262967240983882162764690376671538178 9

n = p * q

e = 8183663731883073888358222525691815926379759515614960280024999622293271099878786578404310708501017635162183389465400464346988336773535405845322737119449928644238198644706155047769786418617062856035359636991144279709706232628631716 9
```

Berechnen Sie den geheimen Schlüssel `d`.

Eine geheime Nachricht besteht aus einem ASCII-Text, der mit der folgenden Funktion `zahl` in eine Zahl umgewandelt wird (die mathGUIde-Funktion `text` wandelt die Zahl wieder in Text um):

```
def zahl(text):
    n = 0
    for c in text:
        n = 256 * n + ord(c)
    return n
```

```
def text(zahl):
    t = ""
    while zahl > 0:
        t = chr(zahl % 256) + t
        zahl //= 256
    return t
```

Die so erhaltene Zahl wurde dem RSA-Algorithmus mit dem geheimen Schlüsselpaar (d,e) übergeben. Das Ergebnis ist die Zahl

```
c =
8348315183984809583210253883546809241083575649043260721465133284770917826175987534248246959569724667055687428470013197977056945532835112416415399111876408517381865703727047595499492835567298234748060640667705079101760348651011236 59
```

Entschlüsseln Sie diese Zahl mit dem öffentlichen Schlüsselpaar (e,n) und wandeln sie das Ergebnis mit der Funktion `text` in den ursprünglichen Text um.

Abgabe in Ihrer Übungsgruppe am 09./10./13. Dezember 2010