Kryptographie - Algebraischer Hintergrund
Prof . Dr. F.-O. Schreyer
Übungsblatt 2: Faktorisierung und RSA

Abgabetermin 14.5.2002
Voraussetzungen: Vorlesungskapitel RSA und Wiederholung, Faktorisierung.

1. Zeichnen Sie folgende Funktionen:
   (a) $g_1 : [1, 11] \to \mathbb{R}$
   $g_1(k) = L_{2^k}\left[\frac{1}{2}, 1\right]$
   (b) $g_2 : [1, 11] \to \mathbb{R}$
   $g_2(k) = L_{2^k}[0, 4]$
   (c) $g_3 : [1, 11] \to \mathbb{R}$
   $g_3(k) = L_{2^k}\left[1, \frac{1}{2}\right]$

2. Faktorisieren Sie die Zahlen
   (a) 510511
   (b) 5302555407858282827768779093
   (c) 713623837172067545560252416065537
   (d) 42144985531257745681402189153111135
   (e) 12098743833798169067520000007523445343024140716896711111
   (f) 64898518442585961302416669382254503060920596574980..
   ..25293841379902123372605065112731390344140051162106..
   ..64274752968417922051839654930184534182840779371249..
   ..77201178904854777462019451974017116414724852487815..
   ..16800000000000000001
   (g) 2468001160766705452066353134549702698515108744549..
   ..4665685615343871770215418328461561352271369287472..
   ..2894942800453480535296312038337227963302750841644..
   ..8080849156722646366456990845503383352913528008289..
   ..3217698465676926977153625636105890357806909711920..
   ..3632383280760251916550382742710343646274895445668..
   ..7336461016448159044677999713509355259225543554112..
   ..18912810182987654354678009876500011111111200611

   mit Probedivision, Pollards $(p-1)$-Methode und mit dem Quadratischen Sieb (soweit jeweils anwendbar).

3. Entschlüsseln Sie die mit RSA verschlüsselte Nachricht:

   `289408762005888076148804447152578040991766697073 81..`

   `..183420407255369817920711693155732712036110954 29446..`

   `..911017127550665279755657138410273668464931091 70684`

   Der öffentliche Schlüssel ist:

   n =`33452526613163807108170062053440751665152000000000100..`

   `00000000000000000000000000000000000000000000000893182..`

   `46057147364978814065682686806945955840000000267`

   e =`65537`

   Die Nachricht wurde im Alphabet $\{A..Z\} \simeq \mathbb{Z}/26$ kodiert durch

$$
\begin{aligned}
A &\mapsto 00 \\
B &\mapsto 01 \\
&\vdots \\
Y &\mapsto 24 \\
Z &\mapsto 25
\end{aligned}
$$

   und die dann erhaltene Zahl mit RSA verschlüsselt.

Die zu faktorisierenden Zahlen, die RSA-Nachricht und der öffentliche Schlüssel können separat als Textdatei heruntergeladen werden von

www.math.uni-sb.de/˜ag-schreyer/krypto/blatt2.txt