Gregor Leander
7.07.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Lösungsvorschläge zum Übungsblatt 3

Aufgabe 1: Random Squares

A. Zuerst berechnet und faktorisiert man die Quadrate der gegebenen Zahlen in $\mathbb{Z}_n$. Die verwendete (und um größere Primzahlen erweiterte) Basis ist $B = [2, 3, 5, 7, 11, 13, 19, 67, 73]$:

$$\begin{array}{lrcrcrcl}
(1) & 1227^2 & \text{mod} & 1504229 & = & 1300 & = & 2^2 \cdot 5^2 \cdot 13 \quad \Rightarrow \quad (0,0,0,0,0,1,0,0,0) \\
(2) & 6165^2 & \text{mod} & 1504229 & = & 401500 & = & 2^2 \cdot 5^3 \cdot 11 \cdot 73 \quad \Rightarrow \quad (0,0,1,0,1,0,0,0,1) \\
(3) & 2138^2 & \text{mod} & 1504229 & = & 58357 & = & 13 \cdot 67^2 \quad \Rightarrow \quad (0,0,0,0,0,1,0,0,0) \\
(4) & 3503^2 & \text{mod} & 1504229 & = & 237177 & = & 3^2 \cdot 19^2 \cdot 73 \quad \Rightarrow \quad (0,0,0,0,0,0,0,0,1) \\
(5) & 83013^2 & \text{mod} & 1504229 & = & 285120 & = & 2^6 \cdot 3^4 \cdot 5 \cdot 11 \quad \Rightarrow \quad (0,0,1,0,1,0,0,0,0)
\end{array}$$

(Für den Algorithmus reicht es, den Exponentenvektor $\bmod 2$ zu speichern.) Aus den Relationen (1) und (3) erhält man:

$$(1227 \cdot 2138)^2 \equiv (\underbrace{2 \cdot 5 \cdot 13 \cdot 67}_{8710})^2 \bmod N$$

Nun kann man N faktorisieren:

$$\begin{aligned}
gcd(1227 \cdot 2138 + 8710, N) &= \underline{1459} \\
gcd(1227 \cdot 2138 - 8710, N) &= \underline{1031}
\end{aligned}$$

Wenn man es hingegen mit den Relationen (2), (4) und (5) versucht erhält man folgendes, unbrauchbares Ergebnis:

$$\begin{aligned}
gcd(6165 \cdot 3503 \cdot 83013 - \sqrt{401500 \cdot 237177 \cdot 285120}) &= 1 \\
gcd(6165 \cdot 3503 \cdot 83013 + \sqrt{401500 \cdot 237177 \cdot 285120}) &= 1504229 = N
\end{aligned}$$

Dies muss irgendwann geschehen: die Erfolgswahrscheinlichkeit für die nichttriviale Zerlegung ist $> 1/2$ aber nicht 1. Selbstverständlich gilt auch für $n|(x+y)$ beziehungsweise $n|(x-y)$ die Gleichung $(x+y)(x-y) \bmod n$.

B. (i) Die gewählte Faktorbasis ist im Folgenden $B = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37]$. Man hätte genauso gut eine andere Faktorbasis wählen können. Zuerst berechnet und faktorisiert man wieder die Quadrate, hier exemplarisch für $1 \leq k \leq 3$ und $0 \leq j \leq 9$:

$k=1$	z_1	$\equiv 417^2 \bmod 173441$	$\equiv 448$	$= 2^6 \cdot 7$	
	z_2	$\equiv 418^2 \bmod 173441$	$\equiv 1283$	$=$	1283
	z_3	$\equiv 419^2 \bmod 173441$	$\equiv 2120$	$= 2^3 \cdot 5$	$\cdot 53$
	z_4	$\equiv 420^2 \bmod 173441$	$\equiv 2959$	$= 11$	$\cdot 269$
	z_5	$\equiv 421^2 \bmod 173441$	$\equiv 3800$	$= 2^3 \cdot 5^2 \cdot 19$	
	z_6	$\equiv 422^2 \bmod 173441$	$\equiv 4643$	$=$	4643
	z_7	$\equiv 423^2 \bmod 173441$	$\equiv 5488$	$= 2^4 \cdot 7^3$	
	z_8	$\equiv 424^2 \bmod 173441$	$\equiv 6335$	$= 5 \cdot 7$	$\cdot 181$
	z_9	$\equiv 425^2 \bmod 173441$	$\equiv 7184$	$= 2^4$	$\cdot 449$
	z_{10}	$\equiv 426^2 \bmod 173441$	$\equiv 8035$	$= 5$	$\cdot 1607$
$k=2$	z_{11}	$\equiv 589^2 \bmod 173441$	$\equiv 39$	$= 3 \cdot 13$	
	z_{12}	$\equiv 590^2 \bmod 173441$	$\equiv 1218$	$= 2 \cdot 3 \cdot 7 \cdot 29$	
	z_{13}	$\equiv 591^2 \bmod 173441$	$\equiv 2399$	$=$	2399
	z_{14}	$\equiv 592^2 \bmod 173441$	$\equiv 3582$	$= 2 \cdot 3^2$	$\cdot 199$
	z_{15}	$\equiv 593^2 \bmod 173441$	$\equiv 4767$	$= 3 \cdot 7$	$\cdot 227$
	z_{16}	$\equiv 594^2 \bmod 173441$	$\equiv 5954$	$= 2 \cdot 13$	$\cdot 229$
	z_{17}	$\equiv 595^2 \bmod 173441$	$\equiv 7143$	$= 3$	$\cdot 2381$
	z_{18}	$\equiv 596^2 \bmod 173441$	$\equiv 8334$	$= 2 \cdot 3^2$	$\cdot 463$
	z_{19}	$\equiv 597^2 \bmod 173441$	$\equiv 9527$	$= 7$	$\cdot 1361$
	z_{20}	$\equiv 598^2 \bmod 173441$	$\equiv 10722$	$= 2 \cdot 3$	$\cdot 1787$
$k=3$	z_{21}	$\equiv 722^2 \bmod 173441$	$\equiv 961$	$= 31^2$	
	z_{22}	$\equiv 723^2 \bmod 173441$	$\equiv 2406$	$= 2 \cdot 3$	$\cdot 401$
	z_{23}	$\equiv 724^2 \bmod 173441$	$\equiv 3853$	$=$	$\cdot 3853$
	z_{24}	$\equiv 725^2 \bmod 173441$	$\equiv 5302$	$= 2 \cdot 11$	$\cdot 241$
	$\ldots$				

Wenn man nun alle Ergebnisse aus der Tabelle entfernt, die nicht über der Faktorbasis zerfallen und sich auf die tatsächlich benötigten Primzahlen beschränkt, erhält man die folgende Tabelle, wobei z_5, z_{11} und z_{12} keine passenden Partner haben:

k		2	3	5	7	13	19	29	31
1	$\mathbf{z_1}$	6	0	0	1	0	0	0	0
	z_5	3	0	2	0	0	1	0	0
	$\mathbf{z_7}$	4	0	0	3	0	0	0	0
2	z_{11}	0	1	0	0	1	0	0	0
	z_{12}	1	1	0	1	0	0	1	0
3	$\mathbf{z_{21}}$	0	0	0	0	0	0	0	2

Man erhält nun die Faktorisierung:

$$gcd(417 \cdot 423 \pm \sqrt{z_1 z_7}, N) = \begin{cases} 251 \\ 691 \end{cases}$$

Oder Alternativ:

$$gcd(722 \pm \sqrt{z_{21}}, N) = \begin{cases} 251 \\ 691 \end{cases}$$

Im Sinne einer effizienten Implementation hätte man die Exponentenvektoren mod 2 speichern müssen, hier wurde der Übersichtlichkeit halber darauf verzichtet.

(ii) Da $\lceil \sqrt{kN} \rceil = \sqrt{kN} + \epsilon$ mit $0 < \epsilon < 1$ gilt, kann man $\left(\lceil \sqrt{kN} \rceil + j \right)^2 \bmod N$ folgendermassen abschätzen

$$\begin{aligned} \left(\lceil \sqrt{kN} \rceil + j \right)^2 \bmod N &= \left(\sqrt{kN} + \epsilon + j \right)^2 \bmod N \\ &= \left(kN + \epsilon^2 + j^2 + 2\sqrt{kN}\, j + 2\,\epsilon\sqrt{kN} + 2\,\epsilon\, j \right) \bmod N \\ &= \epsilon^2 + j^2 + 2\sqrt{kN}\, j + 2\,\epsilon\sqrt{kN} + 2\,\epsilon\, j \end{aligned}$$

und, unter der Annahme, dass k und j ausreichend klein sind, dies ist

$$= O(\sqrt{N})$$

Dies erhöht die Wahrscheinlichkeit, dass die $z_{k,j}$ über der Faktorbasis zerfallen, erheblich. Alternativ kann man die Faktorbasis reduzieren und spart damit Probedivisionen. Man kann somit relativ gezielt nach z_i suchen. Für kryptographische Anwendungen, bei denen 1024 Bit zahlen faktorisiert werden sollen, sind die z_i trotzdem noch ca. 512 Bit lang. Daher stellt diese Verbesserung keine Gefahr für RSA mit einer ausreichenden Schlüssellänge dar.

Aufgabe 2: Faktorisieren mit Kettenbrüchen

A. $N = 53953$

$$\sqrt{N} = \underline{\langle 232; 3, 1, 1, 2, 41, 1, 5, 2, 1, 1, 2, 1, 1, 3, \ldots \rangle}$$

B. Die Rekursionsgleichungen liefern die ersten 15 Näherungsbrüche:

i	q_i	n_i	d_i
0	232	232	1
1	3	697	3
2	1	929	4
3	1	1 626	7
4	2	4 181	18
5	41	173 047	745
6	1	177 228	763
7	5	1 059 187	4 560
8	2	2 295 602	9 883
9	1	3 354 789	14 443
10	1	5 650 391	24 326
11	2	14 655 571	63 095
12	1	20 305 962	87 421
13	1	34 961 533	150 516
14	3	125 190 561	538 969

C. Aus dem Beweis der inversen Kettenbruchentwiklung weiß man, dass

$$n_k d_{k-1} - n_{k-1} d_k = (-1)^{k-1}$$

gilt. Wenn man auf beiden Seiten durch $d_k d_{k-1}$ teilt, erhält man:

$$\frac{n_k}{d_k} - \frac{n_{k-1}}{d_{k-1}} = \frac{(-1)^{k-1}}{d_k d_{k-1}}$$

Nun muss man für k zwei Fälle unterscheiden:

Fall k gerade: Daraus folgt $\frac{n_k}{d_k} \leq \sqrt{N} < \frac{n_{k-1}}{d_{k-1}}$. Somit erhält man:

$$0 \geq \frac{n_k}{d_k} - \sqrt{N} > \frac{-1}{d_k d_{k-1}}$$

Also erhält man:

$$\sqrt{N} - \frac{n_k}{d_k} < \frac{1}{d_k d_{k-1}}$$

Fall k ungerade: Daraus folgt $\frac{n_k}{d_k} \geq \sqrt{N} > \frac{n_{k-1}}{d_{k-1}}$. Somit erhält man:

$$\frac{n_k}{d_k} - \sqrt{N} < \frac{1}{d_k d_{k-1}}$$

Beide Fälle kann man zu

$$\left|\frac{n_k}{d_k} - \sqrt{N}\right| < \frac{1}{d_k d_{k-1}}$$

zusammenfassen. Da $d_k \geq d_{k-1}$ immer gilt, kann man die Abschätzung etwas abschwächen und erhält das Ergebnis:

$$\left|\frac{n_k}{d_k} - \sqrt{N}\right| < \frac{1}{d_k^2}$$

□

D. Man hat:

$$|n_k^2 - N d_k^2| = d_k^2 \left|\frac{n_k^2}{d_k^2} - \sqrt{N}^2\right| = d_k^2 \underbrace{\left|\frac{n_k}{d_k} - \sqrt{N}\right|}_{<\frac{1}{d_k^2}} \cdot \left|\frac{n_k}{d_k} + \sqrt{N}\right| < \left|\frac{n_k}{d_k} + \sqrt{N}\right|$$

Da $\frac{n_k}{d_k}$ gegen $\sqrt{N}$ konvergiert erhält man $|n_k^2 - N d_k^2| < 2\sqrt{N}$ und somit die Behauptung

$$|n_k^2 - N d_k^2| = O(\sqrt{N}) \ . \qquad \square$$

E.

$$\begin{array}{rcrcrl} n_0^2 & = & 232^2 & \equiv & -129 & \mod N \\ n_1^2 & = & 697^2 & \equiv & 232 & \mod N \\ n_2^2 & = & 929^2 & \equiv & -207 & \mod N \\ n_3^2 & = & 1626^2 & \equiv & 179 & \mod N \\ n_4^2 & = & 4181^2 & \equiv & -11 & \mod N \\ n_5^2 & = & 173047^2 & \equiv & 384 & \mod N \\ n_6^2 & = & 177228^2 & \equiv & -73 & \mod N \\ n_7^2 & = & 1059187^2 & \equiv & 169 & \mod N \end{array}$$

Beobachtung: Die Reste sind klein! Sehr klein! Dies bestätigt eine Folgerung der Relation $|n_k^2 - N d_k^2| = O(\sqrt{N})$ aus Teil **D**, nähmich, dass $n_k^2 \bmod N = O(\sqrt{N})$. Sie lassen sich also relaiv einfach faktorisieren. Wenn man -1 in die Faktorbasis aufnimmt, erhält man zusätzliche Relationen.

Man beachte nun, dass man mit den Rekursionsrelationen n_k und d_k modulo N rechnen kann: $\hat{n}_0 = q_0$, $\hat{n}_1 = q_0 q_1 + 1$, $\hat{d}_0 = 1$, $\hat{d}_1 = q_1$ und

$$\hat{n}_i = q_i \hat{n}_{i-1} + \hat{n}_{i-2} \bmod N, \qquad \hat{d}_i = q_i \hat{d}_{i-1} + \hat{d}_{i-2} \bmod N \ .$$

Wir betrachten nun $\hat{n}_i$ und $\hat{n}_i^2 \bmod N$.

F. Es gelten $\hat{n}_7 = 34080$ und $\hat{n}_7^2 \equiv 169 = 13^2 \bmod N$. Daraus ergibt sich:

$$ggT(53953, 34080 \pm 13) = \begin{cases} 331 \\ 163 \end{cases}.$$

In diesem Beispiel hätte man zwar auch $n_7^2 = 1059187^2 \equiv 169 \bmod N$ verwenden können, allerdings ist bei längeren Zahlen besser, stets die n_i modulo N zu reduzieren (dies ist eine Idee von Montgomery).
