Gregor Leander
7.07.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Lösungsvorschläge zum Übungsblatt 4

Aufgabe 1: Quadratwurzeln modulo p

Eine erste Möglichkeit, um n zu wählen, ist $n = 2 \bmod 9941$. Die Werte α und s ergeben sich zu $p - 1 = 9940 = 2^\alpha \cdot s = 2^2 \cdot 2485$ und somit $\alpha = 2$ und $s = 2485$. Nun kann man b und r ermitteln:

$$\begin{aligned} b &\equiv n^s \bmod p \equiv 141 \bmod 9941 \\ r &\equiv a^{\frac{s+1}{2}} \bmod p \equiv 3333 \bmod p \equiv 382 \end{aligned}$$

Jetzt bleibt die Berechunung von j_0, so dass $x = b^{j_0} r$ eine Lösung der Gleichung

$$x^2 = 4792 \bmod 9941$$

ist. Hierfür berechnen wir

$$k = \left(\frac{r^2}{a}\right)^{2^{\alpha-2}} = \left(\frac{r^2}{a}\right) \equiv 1 \bmod 9941$$

und damit ist $j_0 = 0$. Die beiden Lösungen der Gleichug sind somit

$$x = \pm 3333 \bmod 9941$$

Aufgabe 2: Quadratwurzeln modulo n

1. Die beiden Primzahlen kann man noch einfach (zum Bsp. mit Probedivision) finden. Es gilt
$$n = 137238091 = 9241 \cdot 14851$$

2. Man bestimmt zuerst mit dem Verfahren aus Aufgabe 1 die zwei Quadratwurzeln modulo $p = 9241$ und dann die zwei Quadratwurzeln modulo $q = 14851$. Für die Lösungen der Gleichung
$$x^2 = 113050492 \bmod n$$

ergibt sich somit

$$\begin{aligned} x &= \pm 5805 \bmod p \\ x &= \pm 3719 \bmod q. \end{aligned}$$

Diese Lösungen können nun mit dem CRT zusammengesetzt werden und es ergeben sich folgende 4 Möglichkeiten für $x \bmod n$.

$$\begin{aligned} x &= 110435755 \bmod n \\ x &= 87654321 \bmod n \\ x &= 49583770 \bmod n \\ x &= 26802336 \bmod n. \end{aligned}$$

Aufgabe 3: Quadratwurzeln modulo p^t

Gesucht ist eine Methode, um aus gegebenen $a,\ p,\ t$ wobei $p \in \mathbb{P} \setminus \{2\}$ und $\left(\frac{a}{p}\right) = 1$ gelten, ein x zu berechnen, so dass $x^2 \equiv a \bmod p^t$ gilt. Als Hinweis war gegeben, dass man $x = x_0 + x_1 p + x_2 p^2 + \ldots + x_{t-1} p^{t-1}$ in seiner p-adischen Darstellung betrachten soll. Das Verfahren zum Berechenen von Quadratwurzeln mod$p$ (also $t = 1$) ist bereits bekannt.
Da bekannt ist, wie man x_0 findet, benötigt man nur einen Algorithmus, der aus

$$\tilde{x}_i^2 = (x_0 + x_1 p + \ldots + x_{i-1} p^{i-1})^2 \equiv a \bmod p^i$$

ein

$$\tilde{x}_{i+1}^2 \equiv a \bmod p^{i+1}$$

berechnet. Man zeigt nun, dass es immer ein $0 \leq x_i < p$ gibt, so dass

$$\tilde{x}_{i+1}^2 = (\tilde{x}_i + x_i p^i)^2 \equiv a \bmod p^{i+1}$$

gilt. Offensichtlich gelten

$$(\tilde{x}_i + x_i p^i)^2 = \tilde{x}_i^2 + \underbrace{2\tilde{x}_i x_i p^i + (x_i p^i)^2}_{\equiv 0} \equiv a \bmod p^i$$

und:

$$(\tilde{x}_i + x_i p^i)^2 = \tilde{x}_i^2 + 2\tilde{x}_i x_i p^i + \underbrace{(x_i p^i)^2}_{\equiv 0} \equiv a \bmod p^{i+1}$$

Dies löst man nach x_i auf:

$$x_i \equiv \frac{a - \tilde{x}_i^2}{p^i} (2\tilde{x}_i)^{-1} \bmod p^{i+1}$$

Der Bruch lässt sich in $\mathbb{Z}$ berechnen, da $\tilde{x}_i^2 \equiv a \bmod p^i$ und somit $p^i \mid a - \tilde{x}^2$ gilt. $(2\tilde{x}_i)^{-1} \bmod p^{i+1}$ existiert, da sowohl $ggT(2, p^{i+1}) = 1$ (siehe Startbedingung) als auch $ggT(\tilde{x}_i, p^i) = 1$ (siehe p-adische Entwicklung von $\tilde{x}_i$) gelten. Aus $\tilde{x}_{i+1} \equiv \tilde{x}_i \bmod p_i$ und

$$\tilde{x}_{i+1}^2 \equiv a \bmod p^{i+1} \;\Rightarrow\; (\tilde{x}_{i+1}^2 \bmod p^i) \equiv (a \bmod p^i)$$

folgt, dass die Behauptung stimmt. Der Algorithmus lautet:

Algorithm 1. Hensel'sche Hebung

INPUT: quadratischer Rest a und Modulus p^t mit $p \in \mathbb{P} \setminus \{2\}$
OUTPUT: $\tilde{x}$, so dass $\tilde{x}^2 \equiv a \bmod p^t$

---

1. Berechne x_0 mit $x_0^2 \equiv a \bmod p$
2. $\tilde{x} \leftarrow x_0$
3. **for** $i = 1$ **to** $t - 1$ **do**
4. $\quad t \leftarrow (2\tilde{x})^{-1} \bmod p^i$
5. $\quad x_i \leftarrow \left(\frac{a - \tilde{x}^2}{p^i}\right) t \bmod p^i$
6. $\quad \tilde{x} \leftarrow \tilde{x} + x_i p^i$
7. **return** $(\tilde{x})$

Die Überlegungen zu diesem Algorithmus entsprechen in etwa dem Hensel'schen Lemma.
