TECHNISCHE UNIVERSITÄT BERLIN WS09/10
Fakultät II – Institut für Mathematik
Dozent: Tobias Finis
Assistent: Gerriet Möhlmann
www.math.tu-berlin.de/~kant/kryptows09

8. Übung Kryptographie

1. Aufgabe

Beweist oder widerlegt die folgenden Aussagen:

(a) Für alle $n \in \mathbb{Z}$ gibt es $k, a, b \in \mathbb{Z}^{>0}$, so dass gilt:

$$a^2 - b^2 = kn$$

(b) Für alle $n \in \mathbb{Z}$ gibt es $a, b \in \mathbb{Z}$, so dass gilt:

$$a^2 - b^2 = n$$

Hat diese Aufgabe etwas mit dem quadratischen Sieb zutun?

(5 Punkte)

2. Aufgabe

Sei $n \in \mathbb{N}$ mit $n \equiv \pm 3 \mod 8$ und r_2 die kleinste Zweierpotenz mit $\text{ord}(n \mod r_2) > \log_2^2 n$. Dann gilt $r_2 < 8 \log_2^2 n$.

(5 Punkte)

3. Aufgabe

Sei h eine Funktion, die einen n-Bitstring auf einen m-Bitstring abbildet. Wir können daher h als eine Funktion von $\mathbb{Z}/2^n\mathbb{Z}$ nach $\mathbb{Z}/2^m\mathbb{Z}$ interpretieren.

(a) Ferner seien $n = m$ und $h : \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/2^n\mathbb{Z}$ wie folgt definiert:

$$h(x) := x^2 + ax + b \bmod 2^n.$$

Zeigt, dass es einfach ist zu gegebenem $x_0 \in \mathbb{Z}/2^n\mathbb{Z}$ ein x_1 mit $h(x_0) = h(x_1)$ zu finden. Sowas könnte man eine Kollision nennen. Einfach bedeutet ohne die quadratische Gleichung in $\mathbb{Z}/2^n\mathbb{Z}$ lösen zu müssen und nichts mit rumprobieren.

(b) Es seien nun $n > m$ und $h : \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/2^m\mathbb{Z}$ wie folgt definiert:

$$h(x) := \sum_{i=0}^{d} a_i x^i \bmod 2^m,$$

wobei $a_i \in \mathbb{Z}$ für $0 \leq i \leq d$ sind. Zeigt, dass es einfach ist eine Kollision zu gegebenem $x_0 \in \mathbb{Z}/2^n\mathbb{Z}$ zu finden ohne die Polynomgleichung in $\mathbb{Z}/2^m\mathbb{Z}$ lösen zu müssen.

(5 Punkte)

4. Aufgabe

Programmiert den AKS-Primzahltest und vergleicht seine Laufzeit an Hand einiger Beispiele mit der eures Miller-Rabins.

(5 Punkte)