Gregor Leander
23.06.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Übungsblatt 10

Aufgabe 1 *Nicht Degenerierte Pairings* 10 Punkte

Seien Gruppen G_1 und G_2 mit $|G_1| = |G_2| = p$, p prim, sowie ein Pairing

$$e : G_1 \times G_1 \to G_2$$

gegeben. Wie üblich notieren wir die erste Gruppe additive und die zweite multiplikativ. Zeigen Sie, dass folgende Aussagen äquivalent sind.

1. $P \neq 0 \;\Rightarrow\; e(P,P) \neq 1$
2. $\exists P \neq 0,$ so dass $\; e(P,P) \neq 1$
3. $e(P,Q) = 1 \;\forall Q \quad \Rightarrow\; P = 0$

Aufgabe 2 *Noch ein Pairing* 10 Punkte

Sei q prim und sei $G_1 = (\mathbb{Z}_p, +)$ und G_2 eine Untergruppe von $(\mathbb{Z}_q^*, *)$ mit Ordnung p. Zeigen Sie, dass die Abbildung

$$\begin{aligned} e : G_1 \times G_2 &\to G_2 \\ e(x,y) &= y^x \end{aligned}$$

ein Pairing ist. D.h weisen Sie nach, das e

1. bilinear und
2. nicht degeneriert ist.

Nicht degeneriert sei hier wie folgt definiert:

$$e(P,Q) = 1 \;\forall Q \quad \Rightarrow\; P = 0$$

und

$$e(P,Q) = 1 \;\forall P \quad \Rightarrow\; Q = 1.$$

(Siehe dazu auch die erste Aufgabe.)

Abgabe: Freitag, 27.06.2008 bis 12:00 Uhr im Kasten im Gebäude NA Ebene 02 oder Samstag, 28.06.2008 bis 12:00 Uhr per Mail an `mansour.alsawadi@rub.de`.