

Kryptographie II

Übungsblatt 10

Abgabe bis Dienstag, 4.7.2006 NA 5/75.

Aufgabe 1 *DDH mit Pairings*

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

$$e : G_1 \times G_1 \rightarrow G_2$$

gegeben. Zeigen Sie, dass das DDH-Problem in der Gruppe G_1 leicht zu lösen ist.

Aufgabe 2 *Nicht Degenerierte Pairings*

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

$$e : G_1 \times G_1 \rightarrow G_2$$

gegeben. Wie üblich notieren wir die erste Gruppe additiv 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. $e(P, Q) = 1 \forall Q \Rightarrow P = 0$

Aufgabe 3 *Kleine Untergruppe*

Sei G eine endliche zyklische Gruppe mit einer Untergruppe der Ordnung 3. Finden Sie einen effizienten Algorithmus, der das DDH Problem in G mit guter Wahrscheinlichkeit löst.