Gregor Leander
16.06.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Übungsblatt 9

Aufgabe 1 *Decisional Diffie-Hellman Problem* 10 Punkte

Seien $(G_1, +, 0)$ und $(G_2, \cdot, 1)$ zyklische Gruppen mit einer Paarung $e : G_1 \times G_1 \to G_2$. In der Vorlesung wurde gezeigt, dass das diskrete Logarithmus-Problem (DLP) in G_1 nicht schwerer als das DLP in G_2 ist.
Das *Decisional Diffie Hellman-Problem (DDH-Problem)* ist: Gegeben $g, g^a, g^b \in G$ und einer nichtgeordneten Menge von zwei Elementen $\{x, y\} = \{g^{ab}, g^r\}$ mit $a, b, r \in \mathbb{Z}$, bestimme welches Element in der Menge $\{x, y\}$ ist g^{ab}.
Beweise folgenden Satz: *In der Gruppe G_1 ist das DDH-Problem leicht zu lösen.*

Aufgabe 2 *Folge der Existenz einer kleinen Untergruppe* 5+5 Punkte

1. Sei G eine endliche zyklische Gruppe mit einer Untergruppe der Ordnung 5. Finde einen effizienten Algorithmus, der das DDH Problem in G mit guter Wahrscheinlichkeit löst.

2. Sei nun $G = (\mathbb{Z}_p^*, *) \times (\mathbb{Z}_5, +)$, wobei p eine grosse Primzahl sei ($\log_2 p \approx 1024$). In G ist damit das DL Problem schwer und das DDH Problem leicht. Kann man G für eine Signatur analog zu dem BLS Schema nutzen?

Abgabe: Freitag, 20.06.2008 bis 12:00 Uhr im Kasten im Gebäude NA Ebene 02 oder Samstag, 21.06.2008 bis 12:00 Uhr per Mail an `mansour.alsawadi@rub.de`.