TECHNISCHE UNIVERSITÄT BERLIN WS 2007-2008
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. Florian Heß
Assistent: Osmanbey Uzunkol
`www.math.tu-berlin.de/∼hess/krypto-ws2007`
Abgabe: 19.01.2008
in der Übung

10. Übung Kryptographie

(Gruppenbasierte Kryptographie, DLP, CDH und DDH Probleme)

---

1. Aufgabe

Sei G eine zyklische Gruppe der Primzahlordnung $p > 2$ und $n < p/2$. Seien $g, y \in G$ gleichverteilt zufällig gewählt. Wir definieren $M = \{0, \ldots, n\}$ und $h : M \times M \to G$ durch $(m_0, m_1) \mapsto g^{m_0} y^{m_1}$.

(a) Unter welchen (weiteren) Bedingungen an G ist h kollisionsresistent? Beweisen Sie Ihre Antwort.

(b) Wie kann h dann als Hashfunktion $H : \{0,1\}^* \to G$ verwendet werden?

(5 Punkte)

2. Aufgabe

Beweisen Sie die im Skript genannte Laufzeitabschätzung für den Pohlig-Hellman Algorithmus.

(3 Punkte)

3. Aufgabe

Zeigen Sie, dass es einen Algorithmus gibt, der das DDH in $\mathbb{F}_q^\times$ für q ungerade mit Wahrscheinlichkeit $\geq \frac{3}{4}$ löst. Wie sieht es für Untergruppen von $\mathbb{F}_q^\times$ mit Primzahlordnung aus?

(3 Punkte)

4. Aufgabe

Implementieren Sie den Pollard-Rho Algorithmus.

(5 Punkte)

5. Aufgabe

Implementieren Sie den Pohlig-Hellman Algorithmus.

(5 Punkte)

Hinweis: Die Aufgabe 5 kann bis 25.01.2008 abgegeben werden.