TECHNISCHE UNIVERSITÄT BERLIN WS06/07
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr.F. Heß
WM: Dipl.-Math. M. Wagner
www.math.tu-berlin.de/~hess/krypto-ws2006

10. Übung Kryptographie

1. Aufgabe Elliptische Kurven (4 Punkte)

Sei $E : y^2 = x^3 + ax + b$ eine elliptische Kurve über einem endlichen Körper k und $P \in E(k)$. Bestimmen sie $-P$. Zeigen Sie, dass die Gruppenordnung immer durch 2 teilbar ist, wenn das Polynom $x^3 + ax + b$ eine Nullstelle in k hat. Geben Sie ein Beispiel einer elliptischen Kurve an, deren Gruppenordnung eine Primzahl ist.

2. Aufgabe DDH (4 Punkte)

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. Aufgabe Pohlig-Hellman (4 Punkte)

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

4. Aufgabe Pohlig-Hellman (8 Punkte)

Implementieren Sie den Pohlig-Hellman Algorithmus in KASH3.