TECHNISCHE UNIVERSITÄT BERLIN WS09/10
Fakultät II – Institut für Mathematik
Dozent: Tobias Finis
Assistent: Gerriet Möhlmann
www.math.tu-berlin.de/~kant/kryptows09

13. Übung Kryptographie

1. Aufgabe

Sei $G =< g >$ eine zyklische Untergruppe von $\mathbb{Z}/p\mathbb{Z}$ mit $ord(G) = l \in \mathbb{P}$ und l teilt die Ordnung von $\mathbb{Z}/p\mathbb{Z}$ genau einmal. Will man ein DLP $g^x \equiv b \mod p$ in G mit dem Index Calculus Algorithmus lösen, so wird gesagt, dass man Werte $b^{u_i}g^{v_i}$ mit $b^{u_i}g^{v_i} = \prod_{j=1}^{s} p_j^{e_{i,j}}$ bestimmen soll, um aus denen durch Anwendung von log_g lineare Relationen zu gewinnen. Nun ist aber g kein Erzeuger von $\mathbb{F}_p^\times$, sonderen erzeugt nur eine Untergruppe der Primordnung l. Liegt eine Primzahl p_i der Faktorbasis B nicht in der von g erzeugten zyklischen Gruppe, dann existiert $log_g(p_i)$ auch nicht. Beweist, dass das Verfahren trotzdem funktioniert. Eine Idee dafür wäre, das Problem erstmal in $\mathbb{F}_p^\times =< \gamma >$ zu betrachten, dann existieren zumindest $log_\gamma(p_i)$ für alle $p_i \in B$ und auch $log_\gamma(g)$. Verwendt nun, dass gilt $ord(g) = l$ teilt $p - 1$ aber l^2 nicht.

(5 Punkte)

2. Aufgabe

(a) Bestimmt $E(k)$ für $k = \mathbb{F}_5$ und $E : y^2 = x^3 + x + 1$.

(b) Bestimmt eine elliptische Kurve E über einem endlichen Körper k mit $\#E(k) \in \mathbb{P}$.

(4 Punkte)

3. Aufgabe

Sei $E : y^2 = x^3 + ax + b$ eine elliptische Kurve über einem Körper k.

(a) Zeigt, dass ein Punkt $P = (x, y) \neq \mathcal{O}$ auf der Kurve genau dann die Ordnung 2 hat, wenn $y = 0$ gilt.

(b) Wieviele Punkte der Ordnung 2 kann E maximal besitzen.

(c) Gebt eine Kurve, die die maximale Anzahl an Punkten der Ordnung 2 besitzt, an.

(6 Punkte)

4. Aufgabe

Schreibt ein Programm das zwei Punkte einer elliptischen Kurve über einem endlichen Körper der Charakteristik ungleich zwei oder drei addiert. Zum Testen könnt ihr mit *EllipticCurve(q,[a,b])* in Kash die elliptische Kurve $y^2 = x^3 + ax + b$ über $\mathbb{F}_q$ erzeugen. *RandomPoint()* liefert Punkte auf der Kurve. Wenn ihr mit Elementen aus $\mathbb{F}_q$ rechnen wollen, dann können ihr mit $F := GF(q)$ diesen erzeugen. Mit *Coerce*(F, n) könnt ihr ganze Zahlen n nach F schieben.

(5 Punkte)