TECHNISCHE UNIVERSITÄT BERLIN WS08/09
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. Heß
Assistent: G. Möhlmann
Abgabe: 3.2.09
www.math.tu-berlin.de/~hess/krypto-ws2008

13. Übung Kryptographie

1. Aufgabe

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. Finden sie eine elliptischen Kurve, deren Gruppenordnung eine Primzahl ist (entweder durch ausprobieren oder durch CM-Methode).

(5 Punkte)

2. Aufgabe

Bei der Beschreibung des Index Calculus Algorithmus auf Folie 11 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 S nicht in der von g erzeugten zyklischen Gruppe, dann existiert $log_g(p_i)$ auch nicht. Beweisen Sie, 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 $p_i \in S$ und auch $log_\gamma(g)$. Dann muss man noch verwenden, dass gilt $ord(g) = l$ teilt $ord\,\mathbb{F}_p^\times$ aber l^2 nicht.

(5 Punkte)

3. Aufgabe

Implementieren Sie Ver- und Entschlüsseln mit ElGamal in einer Untergruppe der Einheitengruppe eines Primkörpers. Sie können dazu die Methode zum Berechnen eines Erzeugers der Einheitengruppe verwenden, die sie in *el_g.g* finden.

(4 Punkte)

4. Aufgabe

Implementieren Sie - basierend auf einem Baby Step Giant Step oder einem Pollard Rho - einen Algorithmus, der zu einem von Ihrem ElGamal erzeugten Chiffretext den Klartext berechnet, ohne den geheimen Schlüssel zu nutzen.

(6 Punkte)