RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Enrico Thomae

Hausübungen zur Vorlesung

Kryptanalyse

WS 2010/2011

Blatt 8 / 01. Dezember 2010 / Abgabe bis spätestens 08. Dezember 2010, 10 Uhr (vor der Übung)

AUFGABE 1 (5 Punkte)**:**
Sei $N = 15$ und $E : y^2 = x^3 + x + 1$ eine Kurve über $\mathbb{Z}_{15}$. Zeigen Sie, dass E eine elliptische Kurve aber nicht assoziativ bzgl. der Addition ist. Bestimmen Sie dazu zunächst alle Punkte auf der Kurve.

AUFGABE 2 (3 Punkte)**:**
Berechnen Sie folgende Legendre-Symbole:

$$\left(\frac{131}{211}\right) \text{ und } \left(\frac{1009}{9001}\right).$$

AUFGABE 3 (7 Punkte)**:**

1. Implementieren Sie die $p-1$ Methode wie im Skript beschrieben und verwenden Sie $a = 2$. Benutzen Sie ihren Algorithmus um die Zahl $N = 67030883744037259$ zu faktorisieren. Wählen Sie dabei die Schranke $B = 1000$.

2. Warum funktioniert diese Implementierung nicht um die Mersennezahl $M_{67} = 2^{67} - 1$ zu faktorisieren? Verändern Sie ihren Algorithmus und finden Sie einen Primfaktor von M_{67}.

Hinweis: Sie können die `sage` Programm-Codes per Email direkt an **ilya.ozerov@rub.de** schicken.