RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

Hausübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 8 / 4. Dezember 2011 / Abgabe bis spätestens 11. Dezember 2011, 8:30 Uhr in dem Kasten auf NA 02 oder in der Übung

AUFGABE 1 (6 Punkte)**:**
Sei $N = 15$ und $E : y^2 = x^3 + x + 1$ eine Kurve über $\mathbb{Z}_{15}$.

(a) Zeigen Sie, dass E eine elliptische Kurve ist (Dass $\text{ggT}(N, 6) = 3$ gilt, stört nicht). Bestimmen Sie dann alle Punkte auf der Kurve.

(b) Berechnen Sie $((0, 1) + (7, 6)) + (10, 9)$ sowie $(7, 6) + (10, 9)$ auf dieser Kurve, sofern definiert bzw. den Teiler von N, den dies liefert.

AUFGABE 2 (6 Punkte)**:**
Sei $N = p_1 p_2 \cdots p_\ell$ ein Produkt paarweise verschieder Primzahlen mit $p_i > 3$. Es seien $a, b \in \mathbb{Z}_N$ gegeben mit $\text{ggT}(4a^3 + 27b^2, N) = 1$. Wir betrachten die Elliptische Kurve E über $\mathbb{Z}_N$, definiert durch $y^2 = x^3 + ax + b$ und 3 Punkte $P, Q, R \in E$.
Zeigen Sie, dass $(P + Q) + R = P + (Q + R)$ gilt, falls bei keiner auftretenden Addition der Fall eintritt, dass ein Teiler von N ausgegeben wird.
Hinweis: Verallgemeinern (und beweisen) Sie den Satz "Verträglichkeit der Additionsdefinitionen" aus der Vorlesung auf geeignete Weise und benutzen Sie, dass die Addition auf elliptischen Kurven modulo Primzahlen assoziativ ist.

AUFGABE 3 (8 Punkte)**:**

a) 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 $B = 1000$.

b) 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}.

Bemerkung zu b): Sie können für die Schranke B die Werte von 1000 bis 10000 in 1000er Schritten durchprobieren, bis es funktioniert; wenn das nicht funktioniert, liegt es nicht an B.