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 9 / 08. Dezember 2010 / Abgabe bis spätestens 15. Dezember 2010, 10 Uhr (vor der Übung)

AUFGABE 1 (4 Punkte)**:**
Bestimmen Sie mit Hilfe des POHLIG-HELLMAN Algorithmus den diskreten Logarithmus von 3344 zur Basis 3 in der multiplikativen Gruppe $\mathbb{Z}^*_{24389}$. Notieren Sie ihre Zwischenschritte.

AUFGABE 2 (4 Punkte)**:**
Erweitern Sie den 4 Listen Problem Algorithmus mit $|L_i| = 2^{\frac{n}{3}}$ so, dass Sie das Problem auch für $k \geq 4$ Listen in Zeit und Platz $\widetilde{\mathcal{O}}(2^{\frac{n}{3}})$ lösen können.

AUFGABE 3 (7 Punkte)**:**
Implementieren Sie die ECM-Methode wie im Skript beschrieben. Wählen Sie auch die Schranken B_1 und B_2 wie vorgeschlagen.
Benutzen Sie ihre Implementierung um die Zahl

$$N = 18446744400127067027$$

zu faktorisieren.

Hinweis: In `sage` kann eine elliptische Kurve E modulo N mit der Gleichung

$$y^2 = x^3 + ax + b \tag{1}$$

folgendermaßen erzeugt werden.

```
E = EllipticCurve(Integers(N), [a,b]);
```

Um einen Punkt mit Koordinaten x und y festzulegen benutzen sie in sage

```
P = E(x,y);
```

Wenn bei den Operationen auf der Kurve eine Division durch Null stattfindet, wirft `sage` eine Fehlermeldung in der bereits der Wert N faktorisiert ist. Z.B.

```
ZeroDivisionError: Inverse of 357300153500485080762604 does not exist

(characteristic = 120892582299238795103453 3 = 1073741827*1125899906842679)
```

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