RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Ilya Ozerov

Hausübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 9 / 14. Dezember 2011 / Abgabe bis spätestens 21. Dezember 2011, 10 Uhr in dem Kasten auf NA 02

AUFGABE 1 (5 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.

Hinweis: Beachten Sie, dass 24389 *keine* Primzahl ist. Sie müssen also überlegen, wie man die $p-1$-Methode passend verallgemeinern kann.

AUFGABE 2 (10 Punkte)**:**

a) Führen Sie den Henniger-Shacham Algorithmus zur Faktorisierung von $N = 391 = (110000111)$ bei gegebener partieller Information $p = 1??01$ und $q = ?01?1$ durch. Notieren Sie Ihre Zwischenschritte.

b) Führen Sie den Algorithmus „Fehlerkorrektur“ (siehe Folie 28, Teil 2) zur Faktorisierung von $N = 3233 = (10010100001)$ durch zu gegebenem fehlerhaften $\tilde{p} = 011100$ und $\tilde{q} = 110001$. Verwenden Sie Tiefe $t = 2$ und Distanz $d = 1$. Notiere Sie die Zwischenschritte.

AUFGABE 3 (5 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 = 120892582299238795103 4533 = 1073741827*1125899906842679)
```