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 9 / 11. Dezember 2011 / Abgabe bis spätestens 18. Dezember 2011, 10 Uhr in dem Kasten auf NA 02

**AUFGABE 1** (8 Punkte)**:**

(a) Bestimmen Sie mit Hilfe des Pohlig-Hellman Algorithmus den diskreten Logarithmus von 3 zur Basis 2 in der multiplikativen Gruppe $\mathbb{Z}_{11}^*$ (sofern existent). Notieren Sie ihre Zwischenschritte.

(b) Bestimmen Sie mit Hilfe des Pohlig-Hellman Algorithmus den diskreten Logarithmus von 2011 zur Basis 2 in der multiplikativen Gruppe $\mathbb{Z}_{2527}^*$ (sofern existent). Notieren Sie ihre Zwischenschritte.

Hinweis: Beachten Sie, dass $2527 = 19^2 \cdot 7$ *keine* Primzahl ist. Sie müssen also überlegen, wie man die $p-1$-Methode passend verallgemeinern kann. Mittels des chin. RS kann man das Problem aufteilen (optional). Es empfiehlt sich in jedem Fall, als erstes die Ordnung von 2 (in $\mathbb{Z}_{19^2}^*, \mathbb{Z}_7^*$ bzw. $\mathbb{Z}_{2527}^*$ ) zu bestimmen. Einen Taschenrechner/Computer zu benutzen ist für (b) ratsam.

**AUFGABE 2** (7 Punkte)**:**

(a) Faktorisieren sie $77 = (1001101) = pq$ mit Hilfe der partiellen Information $p = (??1?)$ und $q = (1?1?)$ nach dem Algorithmus von Heninger-Shacham.

(b) Führen Sie den Algorithmus „Fehlerkorrektur“ (siehe Skript) zur Faktorisierung von $N = 3233 = (10010100001)$ durch zu gegebenem fehlerhaften $\tilde{p} = (010111)$ und $\tilde{q} = (111001)$. Verwenden Sie Fensterbreite $t = 2$ und Distanz (maximale Gesamtfehlerzahl pro Fenster) $d = 1$. Notiere Sie die Zwischenschritte (z.B. als Baum).

Bemerkung: Mit der Klammernotation $N = (b_t b_{t-1} \dots b_0)$ ist hierbei die Binärdarstellung $N = b_0 + 2b_1 + 4b_2 + \dots$ gemeint.

**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:* Die Rechung mit elliptischen Kurven ist in sage schon implementiert: 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);
```

Die Gruppe wird additiv geschrieben, d.h. um Punkte $P = E(x, y)$ und $Q = E(x', y')$ via Kurvenaddition zu addieren kann man dann in sage einfach $P + Q$ benutzen (bzw. $n * P$ für $P + P + \ldots + P$, was via schneller Exponentiation ausgeführt wird).

Anmerkung: Wenn bei den Operationen auf der Kurve eine Division durch Null stattfindet, wirft sage eine Fehlermeldung in der bereits der Wert $N$ faktorisiert ist, insofern muss der Fall nicht von Ihnen abgefangen werden. Z.B.:

```
ZeroDivisionError: Inverse of 357300153500485080762604 does not exist

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