Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2018/19
23. Jan. 2019

Übungen zur Vorlesung Kryptographie

Blatt 13

Aufgabe 49

Sei p eine 2048-Bit-Primzahl. Eine ganze Zahl $0 < g < p$ ist bekanntlich genau dann Primitivwurzel modulo p, wenn

$$g^{(p-1)/q} \not\equiv 1 \bmod p \quad \text{für alle Primteiler } q \mid p-1.$$

Dies setzt voraus, dass alle Primteiler von $p-1$ bekannt sind.

Es sei nur bekannt, dass $q_1, \ldots, q_k$ alle Primteiler von $p-1$ mit $q_i < 2^{32}$ sind. Wir setzen

$$\mathfrak{G} := \big\{ g \in \{1, \ldots, p-1\} : g^{(p-1)/q_i} \not\equiv 1 \bmod p \quad \text{für } i = 1, \ldots, k. \big\}$$

Sei $\mathfrak{G}_0 \subset \mathfrak{G}$ die Teilmenge aller $g \in \mathfrak{G}$, die *nicht* Primitivwurzel modulo p sind. Man gebe eine Abschätzung der Fehlerquote $\#\mathfrak{G}_0/\#\mathfrak{G}$ nach oben.

Aufgabe 50

Seien G_1, G_2 endliche (multiplikativ geschriebene) Gruppen und seien $a \in G_1$ bzw. $b \in G_2$ Elemente mit $\operatorname{ord}(a) = k$ und $\operatorname{ord}(b) = \ell$.

Man zeige: Das Element $x := (a, b) \in G_1 \times G_2$ hat die Ordnung

$$\operatorname{ord}(x) = \operatorname{lcm}(k, \ell) \qquad \{\text{lcm} = \text{least common multiple}\}$$

Aufgabe 51

Für $N = 77$ und $N = 91$ bestimme man jeweils alle möglichen Ordnungen von Elementen $x \in (\mathbb{Z}/N)^*$. Wieviele Elemente haben eine gerade Ordnung? Für wieviele $x \in (\mathbb{Z}/N)^*$ mit gerader Ordnung $2s$ ist $w := x^s$ eine nicht-triviale Quadratwurzel aus 1 modulo N, d.h. $w \not\equiv \pm 1 \bmod N$.

---

b.w.

Aufgabe 52

Es sei $N = pq$ ein RSA-Modul (d.h. $p \neq q$ ungerade Primzahlen),

```
N = 48697143071687825227575124459968214250304302320077761701002169896
960849485704086692021913348411277933172290727025164511539882456865776 2
633823481949224455365084853230560766737981940817197657377336299 03
```

(dezimale Schreibweise). Der Verschlüsselungs-Exponent ist $e = 2^{16} + 1 = 65537$. Damit wurde ein ASCII-Text $T = (a_0, a_1, \ldots, a_n)$, $(0 \leqslant a_i < 2^8,\ 2^{8(n+1)} < N)$, wie folgt verschlüsselt: Der Text T wurde als ganze Zahl $x := \sum_{i=0}^{n} a_i \cdot 2^{8i}$ codiert und $y := x^e \bmod N$ berechnet. Es ergab sich

```
y = 40865926432683934720778895359875244260914522965416418885804835051
996229362903953076993429633195502903130656223395149017663493450302086 6
884544742278713743470530888666229348357762501916274048383468283 43
```

Man finde den Klartext, falls folgendes bekannt ist: Das Element $u \in (\mathbb{Z}/N)^*$

```
u = 43489170129308535204728234587115553360876263066466360315223022041
670904143512446611893151867723919033697132847711137154848234988790335 6
681703239942491613313090373823149219597260647085950083611392384 95
```

hat die Ordnung $r =$ `226088571744`.
