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

SS 2009
1. Juli 2009

Algorithmische Zahlentheorie

Übungsblatt 11

Aufgabe 41

Sei $N = pq$ ein RSA-Modul ($p \neq q$ ungerade Primzahlen) und $e \geqslant 3$ ein Verschlüsselungs-Exponent für N, d.h. $\gcd(e, \varphi(N)) = 1$. Mit $\lambda(N) := \operatorname{lcm}(p-1, q-1)$ (lcm = least common multiple) werde d' definiert durch

$$ed' \equiv 1 \bmod \lambda(N).$$

Man zeige, dass d' als Entschlüsselungs-Exponent benutzt werden kann, weil

$$x^{ed'} \equiv x \text{ für alle } x \in \mathbb{Z}/N.$$

Wie verhält sich d' zum Entschlüsselungs-Exponenten d, der durch $ed \equiv 1 \bmod \varphi(N)$ definiert ist?

Aufgabe 42

Sei $N = pq$ ein RSA-Modul und e ein zugehöriger Verschlüsselungs-Exponent. Man beweise, dass die Verschlüsselungs-Funktion

$$E : \mathbb{Z}/N \longrightarrow \mathbb{Z}/N, \quad x \mapsto E(x) = x^e \bmod N$$

genau

$$m := (1 + \gcd(e-1, p-1))(1 + \gcd(e-1, q-1)) \geqslant 9$$

Fixpunkte besitzt, d.h. Elemente $x \in \mathbb{Z}/N$ mit $E(x) = x$.

Aufgabe 43

Man betrachte das Mini-RSA-System mit Modul $N = 63383$ und Verschlüsselungs-Exponent $e = 7$. Dieses RSA-System wurde für eine Ascii-Bigramm-Substitution

$$\mathbb{Z}_{256}^2 \ni (a, b) \longmapsto (a', b') \in \mathbb{Z}_{256}^2$$

benutzt, die durch

$$x := a \cdot 256 + b, \quad y := x^e \bmod N, \quad y = a' \cdot 256 + b'$$

definiert ist. Ein Klartext der Länge 8 Bytes wurde damit verschlüsselt. Man entschlüssele den entstandenen Geheimtext:

```
B2F9 D13C CDC7 2083
```

---

b.w.

Aufgabe 44

a) Man zeige, dass $g = 3$ eine Primitivwurzel modulo der Primzahl $p = 4231$ ist

b) Alice und Bob vereinbaren mit dem Diffie-Hellman-Verfahren einen gemeinsamen Schlüssel bzgl. $(p, g) = (4231, 3)$.
Alice sendet an Bob $a = g^\alpha \equiv 408 \bmod p$ und Bob sendet an Alice $b = g^\beta \equiv 1043 \bmod p$.
Der gemeinsame Schlüssel $K = g^{\alpha\beta}$ wird wie folgt zur Erzeugung eines Byte-Stroms $(u_1, u_2, u_3, \ldots)$, $u_i \in \mathbb{Z}/256$, verwendet: Mit

$$U_i := K^i \bmod p = \sum_{j=0}^{13} b_{ij} 2^j,\ b_{ij} \in \{0, 1\}, \quad \text{sei} \quad u_i := \sum_{j=3}^{10} b_{ij} 2^{j-3}.$$

Bob addiert das Pseudo-One-Time-Pad $(u_1, u_2, \ldots, u_{13})$ mit bitweisem XOR zu einem 13 Byte langen ASCII-Klartext und sendet den entstandenen Geheimtext

```
3DEE 21AE 63A9 7428 8CEB F704 3C
```

an Alice. Man berechne K und entschlüssele den Geheimtext.

Abgabetermin: Freitag, 10. Juli 2009, 14 Uhr, Übungskasten im 1. Stock

Die **Klausur** findet am Freitag, **17. Juli 2009**, 14-16 Uhr statt.

Teilnahmeberechtigt sind alle Übungsteilnehmer,
die sich bis spätestens **10. Juli** per Email dazu voranmelden.

Die Anmeldung zur Klausur ist zu senden an Alexander Niske
Email: `niske@informatik.uni-muenchen.de`
Betreff: `Klausur Algorithmische Zahlentheorie`

In der Email sind folgende Angaben zu machen

```
        Name:
     Vorname:
Geburtsdatum:
  Geburtsort:
```

(Diese Angaben werden für den Übungsschein benötigt.)