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

WS 2018/19
21. Nov. 2018

Übungen zur Vorlesung Kryptographie

Blatt 6

Aufgabe 21

a) Sei t eine natürliche Zahl, so dass die drei Zahlen

$$p_1 := 6t + 1, \quad p_2 := 12t + 1, \quad p_3 := 18t + 1$$

prim sind. Man beweise, dass dann $N := p_1 p_2 p_3$ eine Carmichael-Zahl ist.

b) Man beweise oder widerlege: Für jede Carmichael-Zahl N gilt $N \equiv 1 \bmod 4$.

Aufgabe 22

a) Man zeige: Jede Carmichael-Zahl hat mindestens 3 verschiedene Primfaktoren.

b) Man bestimme die kleinste Carmichael-Zahl, die mehr als 3 Primfaktoren hat.

Aufgabe 23

a) Man beweise: Eine ungerade Zahl $N \geqslant 3$ ist genau dann prim, wenn folgende zwei Bedingungen erfüllt sind:

(i) Für alle zu N teilerfremden Zahlen a gilt

$$a^{(N-1)/2} \equiv \pm 1 \bmod N.$$

(ii) Es gibt wenigstens eine zu N teilerfremde Zahl a mit

$$a^{(N-1)/2} \equiv -1 \bmod N.$$

Man zeige an einem Gegenbeispiel, dass (i) allein nicht ausreicht.

b) Man beschreibe einen auf a) beruhenden probabilistischen Primzahltest. Welche Vor- und Nachteile hat dieser gegenüber dem Solovay-Strassen-Test ?

Aufgabe 24

Seien $p, q \geqslant 3$ teilerfremde ungerade Zahlen, die entweder prim oder Carmichael-Zahlen sind. Sei $N := pq$ und seien e und d natürliche Zahlen mit $ed \equiv 1 \bmod (p-1)(q-1)$. Man zeige

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

Man könnte also (N, e) und (N, d) als öffentlichen bzw. privaten Schlüssel eines RSA-Kryptosystems verwenden. Warum ist es trotzdem vorzuziehen, für p und q echte Primzahlen und nicht Carmichael-Zahlen zu verwenden?