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

WS 2011/12
18. Jan. 2012

Einführung in die Kryptographie

Übungsblatt 6

Aufgabe 21

Sei $N = pq$ ein RSA-Modul und e ein zugehöriger Verschlüsselungs-Exponent, d.h. $\gcd(e, \varphi(N)) = 1$. Sei $\lambda(N) := \operatorname{lcm}(p-1, q-1)$ und d' definiert durch

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

(lcm = least common multiple, kleinstes gemeinsames Vielfaches)

Man zeige, dass man d' als Entschlüsselungs-Exponent verwenden kann, d.h. $x^{ed'} \equiv x \bmod N$ für alle $x \in \mathbb{Z}/N$.

In welcher Beziehung steht d' zum üblichen Entschlüsselungs-Exponenten d, der durch $ed \equiv 1 \bmod \varphi(N)$ definiert ist?

Aufgabe 22

Sei $N = uv$, $u, v \geqslant 3$ ungerade, mit $|u - v| \leqslant \alpha \sqrt[4]{N}$, wobei $\alpha > 0$ eine reelle Konstante ist. Man schätze (als Funktion von α) die Anzahl der Schritte ab, die nötig sind, um N mit dem Fermatschen Algorithmus zu faktorisieren.

Als Beispiel faktorisiere man $N := 16317709$ mit dem Fermatschen Algorithmus.

Aufgabe 23

Sei k eine positive ganze Zahl und p eine Primzahl mit $p > 2k$. Man beweise:

$N := 2kp + 1$ ist genau dann prim, wenn es eine ganze Zahl a gibt mit

$$a^{N-1} \equiv 1 \bmod N \quad \text{und} \quad \gcd(a^{2k} - 1, N) = 1.$$

Aufgabe 24

Man beweise: Eine ungerade Zahl $N \geqslant 1$ ist genau dann prim, wenn folgende beiden Bedingungen erfüllt sind:

(1) $a^{(N-1)/2} \equiv \pm 1$ für alle $a \in \mathbb{Z}$ mit $\gcd(a, N) = 1$,

(2) $a^{(N-1)/2} = -1$ für mindestens ein $a \in \mathbb{Z}$.

Man zeige, dass die Bedingung (2) wesentlich ist, indem man Beispiele zusammengesetzter Zahlen angebe, die nur (1) erfüllen (natürlich mit dem Pluszeichen).