Kryptographie Blatt 5

hhu Düsseldorf
WiSe 2023/24

Abgabe: bis Montag 20.11.2023, vor der Vorlesung

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Aufgabe 1: Zeugen für die Zusammengesetztheit

Zeigen Sie:

(a) Jede Fermatsche Zahl $F_n = 2^{2^n} + 1$ besteht den Miller–Rabin-Test zur Basis 2.

(b) $a = 2$ ist Zeuge für die Zusammengesetztheit von $N = 341$ im Miller–Rabin-Test, nicht aber $a = 10$ für die Zusammengesetztheit von $N = 91$.

(c) Warum gibt es beim Fermat-Test für $N = pq$, $p \neq q$ prim, immer Zeugen, d. h. a mod N, $(a, N) = 1$, mit $a^{N-1} \not\equiv 1\ (N)$?

Aufgabe 2: RSA-Angriff bei schwachem privaten Schlüssel

Für $q < p < 2q$, p, q prim und $N = pq$ gilt $N - \varphi(N) < 3\sqrt{N}$. Ist dann noch $d < N^{1/4}/3$ und $ed \equiv 1\ (\varphi(N))$, so existiert ein $k \in \mathbb{Z}$ mit

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

Wie kann dann der private Schlüssel d ermittelt werden? (Schauen Sie in Kapitel Z22 der Vorlesung ZT I nach.) Was bedeutet dies für die Sicherheit des RSA-Verfahrens?

Aufgabe 3: Faktorisierung mit Quadratsummen

(a) Sei N auf zwei verschiedene Arten in eine Summe von zwei Quadraten zerlegt: $N = s^2 + t^2 = u^2 + v^2$, $s \geq t > 0$, $u \geq v > 0$, $s > u$. Zeigen Sie, dass dann $d := (su - tv, N)$ ein nichttrivialer Teiler von N ist.

(b) Zeigen Sie: Ist $N = pq$ mit $p \equiv q \equiv 1\ (4)$, $p \neq q$, so lässt sich N auf zwei verschiedene Arten als Summe von zwei Quadraten schreiben. (Schauen Sie in Kapitel EZ13 der Vorlesung EinfZT nach.)

(c) Kann mit (b) und (a) ein schnelles Faktorisierungsverfahren beschrieben werden?