Wolfgang K. Seiler
Tel. 2515

A5, C201

28. März 2013

6. Übungsblatt Kryptologie

Aufgabe 1: *(4 Punkte)*
Eine Bank verlangt aus Sicherheitsgründen, daß jede Zahlungsverpflichtung ab einer bestimmten Höhe von mindestens zwei der 200 Direktoren unterschrieben wird. Da sie von ihren Geschäftspartnern nicht verlangen kann, daß diese allein dafür 200 öffentliche Schlüssel speichern, erzeugt sie stattdessen ein einziges Schlüsselpaar, die Unterschrift der Bank für diese Zwecke. Welche Informationen muß sie an ihre Direktoren geben, damit keiner allein, aber jede Kombination aus zwei Direktoren für die Bank unterschreiben kann?

Aufgabe 2: *(6 Punkte)*

a) Für welche Zahlen a mit $2 \leq a \leq 14$ zeigt der gewöhnliche Primzahltest nach Fermat, daß 15 keine Primzahl ist?

b) Für welche Zahlen a mit $2 \leq a \leq 14$ zeigt der Primzahltest nach Miller und Rabin, daß 15 keine Primzahl ist?
Hinweis: Mit dem chinesischen Restesatz können Sie hier viel Rechenzeit sparen!

Aufgabe 3: *(4 Punkte)*
Finden Sie einen Bruch mit höchstens zweistelligem Nenner, der den Bruch $\frac{13579}{24680}$ mit einem Fehler von höchstens einem Tausendstel approximiert!

Aufgabe 4: *(6 Punkte)*
Der private Exponent d zum öffentlichen RSA-Schlüssel

$$(N, e) = (840\,546\,479,\ 365\,420\,087)$$

ist ziemlich klein.

a) Bestimmen Sie d via Kettenbrüche! *Hinweis:* $166\,424\,421^e \equiv 10 \bmod N$

b) Faktorisieren Sie N ausgehend von der Kenntnis der beiden Exponenten d und e!
Hinweis: Ist $de - 1 = 2^r u$ mit ungeradem u, so ist $7^u \equiv 288\,579\,249 \bmod N$.

Abgabe bis zum Freitag, dem 12. April 2013, um 11.55 Uhr