Wolfgang K. Seiler
Tel. 2515

A5, C201

21. Oktober 2010

6. Übungsblatt Kryptologie

Aufgabe 1: *(3 Punkte)*
Eine Bank verlangt aus Sicherheitsgründen, daß jede Zahlungsverpflichtung ab einer bestimmiten 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: *(7 Punkte)*

a) Die Mitarbeiter der Firma *Cheapo Ltd.* verschlüsseln alle Nachrichten mit demselben RSA-Modul $N = 670\,726\,081$, allerdings hat jeder Mitarbeiter seinen eigenen Verschlüsselungsexponenten e. Den gestrigen geheimen Rundbrief erhielt der Mitarbeiter mit $e = 3$ als $c_1 = 467\,587\,679$; der mit $e = 7$ erhielt ihn als $c_2 = 594\,499\,549$. Entschlüsseln Sie den Rundbrief, ohne N zu faktorisieren!

b) Der *Paranoia AG* ist einerseits selbst RSA mit 2 048 Bit noch zu unsicher, andererseits fehlen ihr aber die Mittel, um Primzahlen mit nennenswert mehr als 1 024 Bit effizient zu erzeugen. Sie erzeugt daher eine Tausend-Bit Primzahl p und irgendeine Zufallszahl q mit neun Tausend Bit; daraus bildet sie den Modul $N = pq$ und wählt ein zu $p - 1$ teilerfremdes e. Zeigen Sie, daß die Verschlüsselungsfunktion $m \mapsto m^e \bmod N$ injektiv auf der Menge aller natürlicher Zahlen $0 \leq m < p$ ist, bestimmen Sie die Entschlüsselungsfunktion, und diskutieren Sie mögliche Angriffe!

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 Donnerstag, dem 28. Oktober 2010, um 15.30 Uhr