Wolfgang K. Seiler — A5, C201
Tel. 2515

17. Oktober 2007

6. Übungsblatt Kryptologie

Aufgabe 1: (*5 Punkte*)
Die Firma *Cheapo* verschlüsselt alle Nachrichten mit dem RSA-Modul $N = 670\,726\,081$, allerdings hat jeder Mitarbeiter seinen eigenen Verschlüsselungsexponenten e. Den gestrigen 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!

Aufgabe 2: (*5 Punkte*)
Der *Paranoia AG* ist einerseits auch 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 $N = pq$.

a) Zeigen Sie: Ist $\operatorname{ggT}(e, p-1) = 1$, so ist die Verschlüsselungsfunktion $m \mapsto m^e \bmod N$ injektiv auf der Menge aller natürlicher Zahlen $0 \le m < p$.

b) Wie sieht die Entschlüsselungsfunktion aus?

c) Welche Bedingung muß e mindestens erfüllen, damit das Verfahren keine offensichtlichen Sicherheitsmängel hat?

Aufgabe 3: (*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 mit Hilfe des Kettenbruchalgorithmus!
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 $7^u \equiv 288\,579\,249 \bmod N$.

Aufgabe 4: (*4 Punkte*)
Finden Sie in Analogie zu Bleichenbachers Vorgehensweise zur Fälschung elektronischer Unterschriften eine natürliche Zahl x derart, daß $x^3 \bmod N$ mit der Ziffernfolge 999 990 124 beginnt! Hierbei sei beispielsweise

$$N = 67\,060\,615\,705\,610\,336\,233\,417\,234\,727 \approx 67 \cdot 10^{27}\,.$$

Abgabe bis zum Dienstag, dem 23. Oktober 2007, um 12.00 Uhr