Wolfgang K. Seiler
Tel. 2515

A5, C201

10. Oktober 2007

5. Übungsblatt Kryptologie

Aufgabe 1: (*4 Punkte*)
Die Zahl $N = 2\,147\,713\,027$ ist Produkt der Primzahlen $p = 32\,771$ und $q = 65\,537$. Berechnen Sie für die Nachricht $m = 1\,234\,567\,890$ nur mit Taschenrechner die Verschlüsselung $m^{17} \bmod N$!

Aufgabe 2: (*4 Punkte*)

a) Zeigen Sie: Ist $n = pq$ Produkt zweier ungerader Primzahlen, so gibt es genau vier Zahlen a zwischen 0 und $n-1$ mit $a^2 = 1$!

b) Was gilt, wenn $n = 2p$ das Doppelte einer ungeraden Primzahl ist?

Aufgabe 3: (*4 Punkte*)

a) Für die natürliche Zahl t seien $6t+1, 12t+1$ und $18t+1$ allesamt Primzahlen. Zeigen Sie, daß das Produkt P dieser Zahlen eine Carmichael-Zahl ist!

b) Zeigen Sie: Es gibt $1296t^3$ Zahlen a zwischen 1 und $P-1$, für die P den Fermat-Test besteht.

c) Wie verhält sich die Wahrscheinlichkeit dafür, daß P für eine zufällige Basis a den Fermat-Test besteht, wenn t gegen unendlich geht?

Aufgabe 4: (*4 Punkte*)
Finden Sie via Eratosthenes und Fermat die kleinste Zahl $p > 2^{20}$, die nicht als zusammengesetzt erkannt werden kann!

Aufgabe 5: (*4 Punkte*)
Die Chinese Regional Mainland Derivates 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?

Abgabe bis zum Dienstag, dem 16. Oktober 2007, um 12.00 Uhr