Wolfgang K. Seiler
Tel. 2515

A5, C201

14. Oktober 2010

5. Übungsblatt Kryptologie

Aufgabe 1: *(6 Punkte)*

a) Verschlüsseln Sie die „Nachricht“ $m = 12345$ in einem RSA-System mit den beiden Parametern $N = 29719$ und $e = 5$!

b) Der Modul N ist durch die Primzahl $p = 113$ teilbar. Bestimmen Sie den privaten Exponenten d !

c) Wie viele modulare Quadrierungen und sontige modulare Multiplikationen brauchen Sie, um m zu unterschreiben?
Zur Lösung dieser Aufgabe soll nur ein Taschenrechner verwendet werden!

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 $a^2 \equiv 1 \bmod n$!

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

Aufgabe 3: *(5 Punkte)*

Eine Carmichael-Zahl ist eine natürliche Zahl N mit der Eigenschaft, daß für alle a mit $ggT(a, N) = 1$ gilt: $a^{N-1} \equiv 1 \bmod N$.

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: *(5 Punkte)*

a) Finden Sie via Eratosthenes und Fermat die kleinste Zahl $p > 2^{20}$, die nicht als zusammengesetzt erkannt werden kann!

b) Was sagt der erweiterte Fermat-Test zu dieser Zahl?

Abgabe bis zum Donnerstag, dem 21. Oktober 2010, um 15.30 Uhr