Wolfgang K. Seiler
Tel. 2515

A5, C201

15. März 2013

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 einen privaten Exponenten d !

c) Wie viele modulare Quadrierungen und sonstige modulare Multiplikationen brauchen Sie, um eine Nachricht m zu unterschreiben?
Zur Lösung dieser Aufgabe soll nur ein Taschenrechner verwendet werden; die damit ausgeführten Rechenschritte sollen einzeln beschrieben werden!

Aufgabe 2: *(5 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 Vor- und Nachteile des Verfahrens!

Aufgabe 3: *(4 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 von Rabin und Miller zu dieser Zahl?

Abgabe bis zum Freitag, dem 22. März 2013, um 11.55 Uhr