

13. Oktober 2016

5. Übungsblatt Kryptologie

Aufgabe 1: (6 Punkte)

- Verschlüsseln Sie die „Nachricht“ $m = 12345$ in einem RSA-System mit den beiden Parametern $N = 29719$ und $e = 5$!
- Der Modul N ist durch die Primzahl $p = 113$ teilbar. Bestimmen Sie einen privaten Exponenten d !
- 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)

- Die Mitarbeiter der Firma *Cheapo Ltd.* verschlüsseln alle Nachrichten mit demselben RSA-Modul $N = 670726081$, allerdings hat jeder Mitarbeiter seinen eigenen Verschlüsselungsexponenten e . Den gestrigen geheimen Rundbrief erhielt der Mitarbeiter mit $e = 3$ als $c_1 = 467587679$; der mit $e = 7$ erhielt ihn als $c_2 = 594499549$. Entschlüsseln Sie den Rundbrief, ohne N zu faktorisieren!
- Der *Paranoia AG* ist einerseits selbst RSA mit 2048 Bit noch zu unsicher, andererseits fehlen ihr aber die Mittel, um Primzahlen mit nennenswert mehr als 1024 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: (5 Punkte)

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

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

Bestimmen Sie alle natürlichen Zahlen a für die $a^{14} \equiv 1 \pmod{15}$, so daß also der FERMAT-Test zur Basis a die Zahl 15 nicht als zusammengesetzt erkennt!

Abgabe bis zum Dienstag, dem 18. Oktober 2016, um 15.25 Uhr