Wolfgang K. Seiler
Tel. 2515

A5, C201

8. März 2018

4. Übungsblatt Zahlentheorie

Aufgabe 1: *(4 Punkte)*

a) Zeigen Sie: Ist beim RSA-Verfahren der öffentliche Exponent $e = 3$, $N = pq$ der Modul und $\lambda = \mathrm{kgV}(p-1, q-1)$, so ist genau eine der beiden Zahlen $(1+\lambda)/3$ und $(1+2\lambda)/3$ ganzzahlig, und diese Zahl kann als privater Exponent d verwendet werden.

b) Funktioniert dies auch mit $\varphi(N)$ an Stelle von λ ?

c) Für den RSA-Modul $N = 335466653$ ist $\varphi(N) = 335428380$. Bestimmen Sie die Faktorisierung von N !

Aufgabe 2: *(4 Punkte)*

a) Manche Chipkarten implementieren RSA so, daß sie eine Unterschrift $x^d \bmod pq$ bestimmen, indem Sie zunächst $x^d \bmod p$ und $x^d \bmod q$ berechnen und diese Ergebnisse dann nach dem chinesischen Restesatz zusammensetzen. Warum reduziert dies den Rechenaufwand?

b) Im Experiment wurden solche Karten während der Rechnung gestört, indem man sie Wärme, Mikrowellen oder Magnetfeldern aussetzte, die zwar den Chip nicht zerstörten, aber doch einige Rechenschritte falsch werden ließen. Angenommen, der Chip berechnet auf Grund einer solchen Manipulation zwar $x^d \bmod p$ korrekt, nicht aber $x^d \bmod q$, und er setzt seine beiden Rechenergebnisse korrekt zusammen zu einem Ergebnis u. Wie kann der Empfänger aus der Unterschrift u und dem Text x den privaten Exponenten d bestimmen?

Aufgabe 3: *(6 Punkte)*

Die Firmen `dot.com` und ΕΥΚΛΕΙΔΗΣ oHG beziehen beide ihre RSA-Moduln von der Firma *THRIFTY PRIMES* Inc. Diese erzeugt, getreu ihrem Namen, für beide zusammen nur drei Primzahlen p, q, r und schickt $m = pq = 88051$ an `dot.com` sowie $n = qr = 89197$ an die ΕΥΚΛΕΙΔΗΣ oHG. Beide Firmen verwenden den öffentlichen Exponenten $e = 3$.

a) Verschlüsseln Sie die „Nachricht“ 34159 an `dot.com`!

b) Berechnen Sie die Primzahlen p, q, r und den privaten Exponenten der ΕΥΚΛΕΙΔΗΣ oHG!

c) Unterschreiben Sie die „Nachricht“ 12345 im Namen der ΕΥΚΛΕΙΔΗΣ oHG!
NB: Alle notwendigen Rechnungen lassen sich auf einem Taschenrechner mit mindestens zehn Stellen ausführen. Falls Sie ohne Computer arbeiten, reicht aber bei *c)* eine Formel; der Zahlenwert der Unterschrift muß dann nicht bestimmt werden.

Aufgabe 4: *(6 Punkte)*

a) Berechnen Sie den diskreten Logarithmus von 10 modulo 19 zur Basis 13 !

b) Zeigen Sie, daß es modulo 17 keinen diskreten Logarithmus von 10 zur Basis 13 gibt!

c) p sei eine Primzahl. Für welche $a \in \mathbb{F}_p^\times$ hat jedes $x \in \mathbb{F}_p^\times$ einen diskreten Logarithmus zur Basis a ?

Abgabe bis zum Donnerstag, dem 15. März 2018, um 10.10 Uhr