Wolfgang K. Seiler
Tel. 2515

B6, B4.18

4. Oktober 2019

5. Übungsblatt Kryptologie

Aufgabe 1: *(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.

a) Verschlüsseln Sie die „Nachricht“ 34159 an `dot.com` mit deren öffentlichem Exponenten $e = 3$!

b) Die ΕΥΚΛΕΙΔΗΣ oHG hat den öffentlichen Exponenten $e = 1943$. Bestimmen Sie p, q, r und einen möglichst kleinen privaten Exponenten der ΕΥΚΛΕΙΔΗΣ oHG!

c) Wie viele modulare Quadrierungen und wie viele sonstigen modularen Multiplikationen brauchen Sie, um die „Nachricht“ 12345 im Namen der ΕΥΚΛΕΙΔΗΣ oHG zu unterschreiben?

Aufgabe 2: *(4 Punkte)*

Die *Paranoia AG* hält einerseits selbst RSA mit 2048 Bit noch zu unsicher, andererseits fehlen ihr 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: *(6 Punkte)*

Eine Carmichael-Zahl ist eine natürliche Zahl N mit der Eigenschaft, daß für alle a mit $\mathrm{ggT}(a, N) = 1$ 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?

d) Finden Sie die beiden kleinsten Carmichael-Zahlen der hier betrachteten Form!

Aufgabe 4: *(4 Punkte)*

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

Abgabe bis zum Freitag, dem 11. Oktober 2019, um 11.55 Uhr