Wolfgang K. Seiler
Tel. 2515

B6, B4.08

20. März 2025

5. Übungsblatt Kryptologie

Aufgabe 1:

Eine Carmichael-Zahl ist eine zusammengesetzte 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 N dieser Zahlen eine Carmichael-Zahl ist!

b) Für wie viele $a \in \mathbb{Z}/N$ ist $a^{N-1} \equiv 1 \bmod N$?

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

Aufgabe 2:

Ein privater Schlüssel d zum öffentlichen RSA-Schlüssel (N, e) mit $N = pq$ wurde über den erweiterten Euklidischen Algorithmus so bestimmt, daß $de - k\varphi(N) = 1$ ist, wobei $\varphi(N) = (p-1)(q-1)$ ist und (gemäß Aufgabe 4 des dritten Übungsblatts) $d < \varphi(N)$ und $k < e$ ist.

a) Angenommen, Sie kennen e und d. Wie können Sie dann auf einfache Weise $\varphi(N)$ bestimmen?

b) Wie lassen sich die beiden Primzahlen p und q aus N und $\varphi(N)$ bestimmen?

c) Für den RSA-Schlüssel $(N, e) = (13\,342\,081,\ 7)$ führt obige Vorgehensweise auf den privaten Exponenten $d = 3\,809\,847$. Was ist $\varphi(N)$?

d) Bestimmen Sie, ohne N zu faktorisieren, die privaten Exponenten für die RSA-Schlüssel $(N, 3)$ und $(N, 5)$!

e) Berechnen Sie p und q sowie das kleinste gemeinsame Vielfache λ von $p-1$ und $q-1$!

f) Auf welchen privaten Exponenten für $(N, 7)$ kommt man, wenn man den erweiterten Euklidischen Algorithmus auf e und λ anwendet? Würden *c)* bis *e)* einfacher oder schwieriger, wenn man von $(N, 7)$ und dem so berechneten d ausgeht?

Aufgabe 3:

a) Ein Mathematiker möchte zur Feier seines Geburtstags die Kerzen (eine für jedes Lebensjahr) so auf ausgewählte Geburtstagstorten verteilen, daß die Anzahl auf jeder dieser Torten das Quadrat einer (festen) Primzahl p ist. Bei seinen Versuchen mit $p = 2, 3$ und 5 bleiben dabei aber jeweils p Kerzen übrig. Wie alt wird er?

b) Wie alt müßte er werden, bis ihm dies zum nächsten Mal passiert?

c) Wann ist sein nächster Geburtstag, für den er eine geeignete Primzahl p finden kann?

d) Einige Zeit später versucht er dasselbe bei der Feier zum Geburtstag eines klassischen griechischen Mathematikers. Aus Mangel an Torten kann er hier allerdings nicht mit so kleinen Primzahlen arbeiten und versucht es deshalb mit $p = 7$ und $p = 11$. Wieder bleiben jeweils p Kerzen übrig. Wann wurde der griechische Mathematiker geboren?

Abgabe und Besprechung am Mittwoch, dem 26. März 2025, um 15.30 Uhr