WOLFGANG K. SEILER
Tel. 2515

B6, B4.08

14. Oktober 2022

6. Übungsblatt Kryptologie

Aufgabe 1:

a) Finden Sie mit Hilfe des erweiterten EUKLIDischen Algorithmus zwei möglichst kleine natürliche Zahlen x, y für die $123x - 456y = 33$ ist!

b) Was ist die allgemeine ganzzahlige Lösung dieser Gleichung?

c) Zeigen Sie, daß die Gleichung $123x - 456y = 100$ keine ganzzahlige Lösung hat!

Aufgabe 2:

a) Ein Mathematiker möchte zur Feier seines Geburtstags die Kerzen (eine für jedes Lebensjahr) so auf ausgewählten 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) Einige Zeit 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?

Aufgabe 3:

Der private Schlüssel d zum öffentlichen RSA-Schlüssel (N, e) wird über den erweiterten EUKLIDischen Algorithmus so bestimmt, daß $de - k\varphi(N) = 1$ ist, wobei $N = pq$ ist und $\varphi(N) = (p-1)(q-1)$.

a) Angenommen, Sie kennen e und d. Wie können Sie dann $\varphi(N)$ 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 4:

Eine Chipkarte für elektronische RSA-Unterschriften zum öffentlichen Schlüssel $(58039, 5)$ berechnet $x^d \bmod N$ nach dem chinesischen Restesatz aus $x^d \bmod p$ und $x^d \bmod q$, wobei $N = pq$ ist. Durch eine thermische Störung wird bei der Unterschrift unter die Nachricht 27182 eine der beiden modularen Potenzen falsch berechnet; sodann werden die beiden Ergebnisse korrekt über den chinesischen Restesatz zusammengesetzt. Das Ergebnis ist die Unterschrift 51499. Finden Sie p und q !

Besprechung am Mittwoch, dem 19. Oktober 2022, um 15.30 Uhr