Wolfgang K. Seiler
Tel. 2515

B6, B4.18

28. September 2019

4. Übungsblatt Kryptologie

Aufgabe 1: *(3 Punkte)*

a) Zeigen Sie: Sind a und b teilerfremde natürliche Zahlen, so gibt es ganze Zahlen α, β mit $0 \leq \alpha < b$ und $0 \leq \beta < a$, so daß $\alpha a - \beta b = 1$ ist.

b) p und q seien zwei verschiedene Primzahlen, $p \equiv q \equiv 2 \bmod 3$, $N = pq$, und λ sei das kleinste gemeinsame Vielfache von $p-1$ und $q-1$. Zeigen Sie: Genau eine der beiden Zahlen $(1+\lambda)/3$ und $(1+2\lambda)/3$ ist eine natürliche Zahl d, und die Abbildung $y \mapsto y^d \bmod N$ ist die Umkehrabbildung zu $x \mapsto x^3 \bmod N$.

c) Auch für $d' = \big(1 + 2(p-1)(q-1)\big)/3$ ist $y \mapsto y^{d'} \bmod N$ eine Umkehrabbildung. Welche der beiden sollte man verwenden?

Aufgabe 2: *(4 Punkte)*

a) Finden Sie die Umkehrabbildung zu φ: $\begin{cases} \mathbb{F}_p \to \mathbb{F}_p \\ x \mapsto x^e \end{cases}$ für die Primzahl $p = 123\,456\,791$ und den Exponenten $e = 3$!

b) Zeigen Sie, daß es für $e = 2$ keine Umkehrabbildung gibt!

c) Bestimmen Sie alle $e \leq 10$, für die φ eine Umkehrabbildung hat!

Aufgabe 3: *(8 Punkte)*

a) Zeigen Sie: Für zwei zueinander teilerfremde Zahlen n, m ist die Abbildung von $\mathbb{Z}/mn$ nach $\mathbb{Z}/m \times \mathbb{Z}/n$, die jeder Restklasse $x \bmod mn$ das Paar $(x \bmod m, x \bmod n)$ zuordnet, bijektiv!

b) Wie müßte man RSA modifizieren, wenn man modulo dem Produkt $N = pqr$ von drei verschiedenen Primzahlen arbeiten würde? Welche Bedingung müßte dann der öffentliche Exponent e erfüllen, und wie würde man diesen privaten Exponenten d aus e berechnen?

c) Welche Vor- und/oder Nachteile hätte das so modifizierte RSA-Verfahren gegenüber dem üblichen?

d) Zeigen Sie, daß für $N = 255$ die Abbildung $\mathbb{Z}/N \to \mathbb{Z}/N$ mit $x \mapsto x^e$ für jede ungerade Zahl e bijektiv ist!

e) Bestimmen Sie für $e = 9$ eine möglichst kleine natürliche Zahl d, so daß $x \mapsto x^d$ die Umkehrabbildung zu $x \mapsto x^e$ ist!

Aufgabe 4: *(5 Punkte)*

a) Zeigen Sie: $N = 2^{2n} - 1$ ist genau dann eine Primzahl, wenn $n = 1$ ist.

b) Zeigen Sie: $2^n - 1$ ist genau dann durch drei teilbar, wenn n gerade ist. *Hinweis:* $2 \equiv -1 \bmod 3$

c) Die Zahl $N = \frac{1}{3}(2^{122} - 1)$ ist Produkt zweier Primzahlen. Finden Sie diese **ohne** Computerhilfe!

d) Finden Sie den kleinsten öffentlichen Exponenten e, den man in einem RSA-System mit Modul N benutzen kann!

e) Bestimmen Sie den privaten Exponenten dazu! *(Hierzu sollten Sie zweckmäßigerweise einen Computer benutzen.)*

Abgabe bis zum Freitag, dem 4. Oktober 2019, um 11.55 Uhr