Wolfgang K. Seiler
*Tel.* 2515

A5, C201

*5. Oktober 2016*

# 4. Übungsblatt Kryptologie

**Aufgabe 1:** *(4 Punkte)*

*a)* Finden Sie die Umkehrabbildung zu $\varphi$: $\begin{cases} \mathbb{F}_p \to \mathbb{F}_p \\ x \mapsto x^e \end{cases}$ 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 $\varphi$ eine Umkehrabbildung hat!

**Aufgabe 2:** *(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 $(x \bmod m, x \bmod m)$ 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 3:** *(3 Punkte)*

Leider haben Sie nur eine alte RSA-Implementierung, die nicht mit den heute wünschenswerten Modullängen zurechtkommt. Um trotzdem ein sicheres System zu bekommen, entwickeln Sie in Anlehnung an Triple-DES das folgende Triple-RSA-System: Sie wählen sich einen Modul $N$ und zwei öffentliche Exponenten $e_1, e_2$; ein Block $b$ wird dann verschlüsselt als $\mathrm{RSA}_{N,e_1}\left(\mathrm{RSA}_{N,e_2}\left(\mathrm{RSA}_{N,e_1}(b)\right)\right)$.

*a)* Warum wird in der Mitte nicht, analog zu Triple-DES, $\mathrm{RSA}^{-1}_{N,e_2}$ verwendet?

*b)* Ist die Sicherheit von Triple-RSA vergleichbar mit der von einfachem RSA mit doppelter Blocklänge?

**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! *(Spätestens hierzu sollten sie definitiv einen Computer benutzen!)*

**Abgabe** bis zum Dienstag, dem 11. Oktober 2016, um 15.25 Uhr