Wolfgang K. Seiler
*Tel.* 2515

B6, B4.08

*12. März 2025*

# 4. Übungsblatt Kryptologie

**Aufgabe 1:**

*a)* Zeigen Sie, daß die Kongruenz $a^{n-1} \equiv 1 \bmod n$ nicht gelten kann, wenn $\mathrm{ggT}(a, n) > 1$ ist!

*b)* Bestimmen Sie alle natürlichen Zahlen $a$, für die $a^{14} \equiv 1 \bmod 15$ ist!

**Aufgabe 2:**

$N = pq$ sei das Produkt zweier verschiedener Primzahlen.

*a)* Folgern Sie aus dem kleinen Satz von Fermat, daß die Abbildung $x \mapsto x^e$ von $\mathbb{Z}/N$ nach $\mathbb{Z}/N$ nicht surjektiv sein kann, falls $\mathrm{ggT}(e, p-1) > 1$ ist!

*b)* Zeigen Sie, daß die Abbildung genau dann bijektiv ist, wenn $e$ teilerfremd sowohl zu $p-1$ als auch zu $q-1$ ist!

**Aufgabe 3:**

Bestimmen Sie die Mengen aller ganzer Zahlen $x$, für die die folgenden Kongruenzen erfüllt sind:

*a)* $5x \equiv 7 \bmod 11$ *b)* $3x \equiv 7 \bmod 15$ *c)* $6x \equiv 9 \bmod 15$

**Aufgabe 4:**

*a)* 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?

*b)* Welche Vor- und/oder Nachteile hätte das so modifizierte RSA-Verfahren gegenüber RSA?

*c)* Zeigen Sie, daß $\varphi\colon \mathbb{Z}/255 \to \mathbb{Z}/255$ mit $\varphi(x) = x^e$ für jede ungerade Zahl $e$ bijektiv ist!

*d)* Bestimmen Sie für $e = 9$ eine möglichst kleine natürliche Zahl $d$, so daß $x \mapsto x^d$ die Umkehrabbildung zu $x \mapsto x^e \bmod 255$ ist!

**Aufgabe 5:**

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 $e = 17$!

*b)* Die ΕΥΚΛΕΙΔΗΣ oHG hat den öffentlichen Exponenten $e = 1943$. Bestimmen Sie einen möglichst kleinen privaten Exponenten dazu!

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

**Abgabe und Besprechung** am Mittwoch, dem 19. März 2025, um 15.30 Uhr