Wolfgang K. Seiler
Tel. 2515

B6, B4.08

6. Oktober 2022

5. Übungsblatt Kryptologie

Aufgabe 1:

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 2:

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 p, q, r und einen möglichst kleinen privaten Exponenten der ΕΥΚΛΕΙΔΗΣ oHG!

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

Aufgabe 3:

Die *Paranoia AG* hält einerseits selbst RSA mit drei Tausend Bit noch für zu unsicher, andererseits fehlen ihr die Mittel, um Primzahlen mit nennenswert mehr als Tausend Bit effizient zu erzeugen. Sie erzeugt daher eine Tausend-Bit Primzahl p und irgendeine Zufallszahl q mit neun Tausend Bit; daraus bildet sie den Modul $N = pq$ und wählt ein zu $p - 1$ teilerfremdes e. Zeigen Sie, daß die Verschlüsselungsfunktion $m \mapsto m^e \bmod N$ injektiv auf der Menge aller natürlicher Zahlen $0 \le m < p$ ist, bestimmen Sie die Entschlüsselungsfunktion, und diskutieren Sie Vor- und Nachteile des Verfahrens!

Aufgabe 4:

Für eine Primzahl p ist bekanntlich $a^{p-1} \equiv 1 \bmod p$ für alle zu p teilerfremden ganzen Zahlen a. Ist p zusammengesetzt, kann diese Kongruenz immer noch für manche a gelten.

a) Zeigen Sie: Falls $\mathrm{ggT}(a, p) > 1$ ist, kann die Kongruenz nicht gelten.

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

Aufgabe 5:

Eine Carmichael-Zahl ist eine zusammengesetzte natürliche Zahl N mit der Eigenschaft, daß für alle a mit $\mathrm{ggT}(a, N) = 1$ 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 P dieser Zahlen eine Carmichael-Zahl ist!

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

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

Besprechung am Mittwoch, dem 12. Oktober 2022, um 15.30 Uhr