8. Übung Kryptographie

1. Aufgabe Carmichael-Zahlen

(4 Punkte)

Ein $n \in \mathbb{N}$ heißt **zusammengesetzt** wenn n nicht prim ist. Sei n eine zusammengesetzte ungerade Zahl für die

$$a^{n-1} \equiv 1 \pmod{n}$$

gilt für ein $a \in \mathbb{Z}$. Solch eine Zahl nennt man **Pseudoprimzahl** zur Basis a . Ist n für alle $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$ eine Pseudoprimzahl zur Basis a , so nennt man n **Carmichael-Zahl**. Man nennt $n \in \mathbb{N}$ **quadratfrei**, wenn es kein $p \in \mathbb{P}$ gibt mit $p^2 | n$. Zeige, dass eine Carmichael-Zahl mindestens drei verschiedene Primteiler hat.

Benutze dazu die folgende Aussage ohne Beweis:

$$n \text{ ist Carmichael-Zahl} \Leftrightarrow n \text{ ist quadratfrei und es gilt: } p|n \Rightarrow (p-1)|(n-1) \quad (p \in \mathbb{P}).$$

2. Aufgabe

(4 Punkte)

Ist p eine Primzahl und g ein Erzeuger der multiplikativen Gruppe $G := (\mathbb{Z}/p\mathbb{Z})^\times$, so berechnet man für ein $x \in \{0, 1, \dots, p-2\}$ das Element $y = g^x$. Dieses y ist öffentlich wohingegen x privat ist. Ist nun $m \in G$ eine zu verschlüsselnde Nachricht, so wählt man $r \in \mathbb{Z}$ zufällig und bildet $u := g^r$ und $v := my^r$. Der Chiffretext ist dann (u, v) . Zum Entschlüsseln berechnet man dann $vu^{-x} = my^r g^{-rx} = mg^{rx} g^{-rx} = m$.

- (i) Bestimmen sie alle Erzeuger von von $(\mathbb{Z}/43\mathbb{Z})^\times$.
- (ii) Alice erhält den ElGamal-Chiffretext $(u = 37, v = 24)$. Ihr öffentlicher Schlüssel ist $(p = 43, g = 3)$. Bestimmen Sie den zugehörigen Klartext, wenn $x = 9$ ist.
- (iii) Der öffentliche Schlüssel von Bob sei $p = 53, g = 2, y = 30$. Alice erzeugt damit den Chiffretext $(24, 37)$. Wie lautet der Klartext?

3. Aufgabe Faktorisierung ganzer Zahlen

(4 Punkte)

- (i) Finden Sie einen echten Teiler von $n = 11111$ mit dem quadratischen Sieb.
- (ii) Faktorisieren Sie $n = 138277151$ mit der $p - 1$ -Methode.

4. Aufgabe Miller-Rabin

(8 Punkte)

Implementieren Sie den Miller-Rabin-Test in KASH3.