Kryptologie
Übungsblatt 5

Aufgabe 5.1

Die ersten zwei Carmichael-Zahlen sind $561 = 3 \cdot 11 \cdot 17$ und $1105 = 5 \cdot 13 \cdot 19$. Berechnen Sie die Wahrscheinlichkeit, dass 561 bzw. 1105 bei zufälliger Wahl von $a \in \{2, ..., n-1\}$ den Fermat-Test (fälschlicherweise) besteht.

Aufgabe 5.2

Sei n eine ungerade Primzahl und sei a teilerfremd zu n. Lässt sich folgern, ob a quadratischer Rest oder Primitivwurzel modulo n ist, wenn

(a) $a^{(n-1)/2} \equiv -1 \mod n$ gilt?

(b) $a^{(n-1)/2} \equiv +1 \mod n$ gilt?

Aufgabe 5.3

Zeigen Sie, dass die folgenden beiden Probleme gegenseitig mittels $\preccurlyeq$ reduzierbar sind:

Diffie-Hellman-Problem:

Gegeben:
- n (Primzahl),
- a (Primitivwurzel $\mod n$),
- $\tilde{x}$ ($= a^x \mod n$),
- $\tilde{y}$ ($= a^y \mod n$).

Finde: $z = a^{xy} \mod n$.

El Gamal-System brechen:

Gegeben:
- n (Primzahl),
- a (Primitivwurzel $\mod n$),
- $\tilde{x}$ ($= a^x \mod n$),
- $\tilde{y}$ ($= a^y \mod n$),
- $\tilde{m}$ ($= a^{xy} \cdot m \mod n$).

Finde: m.

Aufgabe 5.4

(a) Seien $f : A \to A$ und $g : A \to A$ beides Einwegfunktionen auf derselben Grundmenge A. Das heißt, $f, g \in \mathrm{P}$, jedoch $f^{-1}, g^{-1} \notin \mathrm{P}$.
Zeigen Sie, dass $h := f \circ g$ ebenfalls eine Einwegfunktion auf A ist. Hierbei ist $g \circ f$ so definiert, dass zuerst f, dann g ausgeführt wird.

(b) Eine *Einwegfunktion mit Falltür* ist eine Einwegfunktion f, so dass es einen effizienten Algorithmus M und für jede Länge n (von y) einen Schlüssel k_n gibt, so dass für alle y der Länge n gilt: $M(y, k_n) = f^{-1}(y)$. Das heißt, für den Berechtigten, der im Besitz des Schlüssels k_n ist, ist es effizient möglich, die Umkehrfunktion von f zu berechnen.
Seien nun $f : A \to A$ und $g : A \to A$ beides Einwegfunktionen mit Falltür auf A. Was können Sie nun über die Verknüpfung $h = g \circ f$ sagen?

Aufgabe 5.5

Für eine gegebene Zahl n haben wir zwei Zahlen x, y gefunden mit $x^2 \equiv y^2 \mod n$, wobei $x \not\equiv \pm y \mod n$ ist. Man zeige, dasss daraus folgt, dass n keine Primzahl sein kann, und dass darüber hinaus $\mathrm{ggT}(x - y, n)$ einen nicht-trivialen Faktor von n ergibt.