Kryptographie *WS 2012/13*
Barbara Baumeister

7. Übungsblatt

Abgabe: Donnerstag, 29.11.2012

Aufgabe 1 (a) Zeigen Sie mit dem Miller-Rabin-Test, dass $n = 99991$ mit Wahrscheinlichkeit größer als $1 - (\frac{1}{4})^4 \approx 0,996$ eine Primzahl ist. (Achtung: n braucht keine Primzahl zu sein)

(b) Wie oft muss der Solovay-Strassen-Test durchgeführt werden, um dieselbe Wahrscheinlichkeit zu erhalten? Führen Sie den Test einmal durch.

Aufgabe 2 Beweisen Sie das Euler'sche Lemma: Ist p eine ungerade Primzahl und teilt p nicht a, dann gilt

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p.$$

Aufgabe 3 Verwenden Sie den Pohlig-Hellman-Algorithmus, um den diskreten Logarithmus von 2 zur Basis 3 mod 65537 zu berechnen.

Aufgabe 4 Beweisen Sie: Genau dann ist $n \in \mathbb{N}$ eine Primzahl, wenn die Kongruenz

$$(n-1)! \equiv -1 \bmod n$$

gilt.
Hinweis: Rechnen Sie in der Gruppe $\mathbb{Z}_n^*$.