Spezielle Aspekte: Kryptographie *SoSe 2011*
Barbara Baumeister

12. Präsenzübungsblatt

Aufgabe 1 (a) Bestimmen Sie die kleinste Primitivwurzel modulo 1117, d.h die kleinste Zahl $a < 1117$ so, dass $a^{1117} \equiv 1 \bmod 1117$ ist, aber $a^k \neq 1$ ist für $k < 1117$.

(b) Bestimmen Sie ein erzeugendes Element von $\mathbb{Z}_{1117}^*$.

Aufgabe 2 Verwenden Sie den Babystep-Giantstep-Algorithmus um den diskreten Logarithmus von 15 zur Basis 2 mod 239 zu berechnen.

Aufgabe 3 Suchen Sie eine Primzahl $p > 60$ und bestimmen Sie $g, h \in \mathbb{Z}_p$ so, dass Sie mit diesen g, h eine Aufgabe aufstellen können, die mit dem Babystep-Giantstep-Algorithmus oder dem Pohlig-Hellman-Algorithmus gelöst werden kann. Schreiben Sie diese Aufgabe auf.

Aufgabe 4 Lösen Sie die Aufgabe 3 von einem anderen Teilnehmer.