Kryptographie *WS 2015/16*
Barbara Baumeister
Tutoren: Apolonia Gottwald, Soeren Senkovic

7. Übungsblatt

Abgabe: Donnerstag, 17.12.2015

Aufgabe 1 Kann $n = 13199$ mit der Methode von Fermat faktorisiert werden?

Aufgabe 2 Faktorisieren Sie $n = 138277151$ mit der $p-1$-Methode von Pollard.

Aufgabe 3 Faktorisieren Sie $n = 5609$ mit der Methode von Dixon und Pommerance.

Aufgabe 4 Sei p eine Primzahl, die kongruent 1 modulo 4 ist. Weiter sei a ein Quadrat in $\mathbb{Z}_p$ und u eine Zahl, die kein Quadrat in $\mathbb{Z}_p$ ist (z.B. falls $p \equiv 5 \bmod 8$, dann können wir $u = 2$ wählen). Zeigen Sie, wie wir mit Hilfe von a und u die Wurzel von a bestimmen können.