Spezielle Aspekte: Kryptographie *SoSe 2011*
PD Dr. Barbara Baumeister
Tutoren: Patrick Wegener, Philipp Neumann, Patrik Odenbach

3. Übungsblatt

Abgabe: Mittwoch, 27.4.11

Aufgabe 1 *Zeigen Sie: Division mit Rest von a durch b, $a, b \in \mathbb{Z}$, benötigt $\mathcal{O}(l(a/b)l(b))$ viel Zeit.*

Aufgabe 2 *Bestimmen Sie mit Hilfe des euklidischen Algorithmus*

(a) *$ggT(1155, 1950)$;*

(b) *Die Lösungen von $122x \equiv 1 \bmod 343$*

Aufgabe 3 *(a)* *Bestimmen Sie mit der eulerschen φ-Funktion $|\mathbb{Z}_{12}^*|$.*

(b) *Bestimmen Sie die Elemente von $\mathbb{Z}_{12}^*$.*

(b) *ZUSATZ: Geben Sie zu jedem $a \in \mathbb{Z}_{12}^*$ sein inverses Element an.*

Aufgabe 4 *Besuche die Seite*

http://www.cryptool-online.org

und probiere die Chiffren CAESAR und VIGNERE aus.