Spezielle Aspekte: Kryptographie *SoSe 2011*
Barbara Baumeister

1. Übungsblatt

Abgabe: Mittwoch, 13.4.11

Aufgabe 1 Stellen Sie die Gruppentafeln von

(a) $(\mathbb{Z}_3, \oplus)$
(b) $(\mathbb{Z}_5, \oplus)$

auf.

Aufgabe 2 Berechnen Sie ohne Taschenrechner 2^{19} mod 7.

Aufgabe 3 HMIWIV XIBX MWX PIMGLX DY IRXWGLPYIWWIPR
Wie wurde verschlüsselt? Welcher Schlüssel wurde verwendet?

Aufgabe 4 Betrachten Sie auf $\mathbb{Z}_m$ die Multiplikation:

$$\overline{a} \odot \overline{b} := \overline{ab} \text{ for } \overline{a}, \overline{b} \in \mathbb{Z}_m.$$

Zeigen Sie an einem Beispiel, dass aus

$$\overline{a} \odot \overline{b} = \overline{a} \odot \overline{c}$$

nicht

$$\overline{b} = \overline{c}$$

folgen muss.