Krypographie mit Gruppen *SoSe 2009*
Barbara Baumeister

2. Übungsblatt

Abgabe: Mittwoch, 13.5.09

Aufgabe 1 (a) Lösen Sie $122x \equiv 1 \bmod 343$.

(b) Sei p eine Primzahl, $p \equiv 3 \bmod 4$. Sei a eine ganze Zahl, die ein Quadrat mod p ist. Zeigen Sie, dass $a^{(p+1)/4}$ eine Quadratzahl von a mod p ist.

Aufgabe 2 Sei g ein Element einer Gruppe G. Wir wollen die Ordnung dieses Elements ermitteln. Dazu wählen wir zufällig k ganze Zahlen e_i, $1 \leq i \leq k$, und berechnen $a_i = g^{e_i}$. Sobald zwei Exponenten e_i und e_j gefunden sind mit $g^{e_i} = g^{e_j}$ ist $g^{e_i - e_j} = 1$, also $e := e_i - e_j$ ein Vielfaches der Ordnung von g. Wenn wir so fortfahren, können wir die Ordnung von g finden. Wie gross muss k sein, damit die Wahrscheinlichkeit, ein solches Vielfaches zu finden, grösser als $1/2$ ist?

Aufgabe 3 (a) Ist die Caesar-Chiffre perfekt sicher?

(b) Gegeben sei ein Kryptosystem mit $\mathcal{P} = \{a, b\}, \mathcal{C} = \{A, B\}, \mathcal{K} = \{0, 1\}$ und Verschlüsselungsfunktionen e_0 und e_1 mit $e_0(a) = A, e_0(b) = B, e_1(a) = B$ und $e_1(b) = A$. Weiter sei auf $\mathcal{P}$ ein Wahrscheinlichkeitsmaß durch $P(a) = \frac{1}{3}$ und $P(b) = \frac{2}{3}$ definiert.
Gibt es ein Wahrscheinlichkeitsmaß auf $\mathcal{K}$, so dass dieses Kryptosystem perfekt sicher ist?

Aufgabe 4 Betrachte die Blockchiffre mit Blocklänge n über dem Alphabet $\sum = GF(q), q$ Primzahlpotenz. Dabei sei sowohl auf dem Klartextraum $\mathcal{P} = \Sigma^n$ als auch auf dem Schlüsselraum $\mathcal{K}$ der $n \times n$-Matrizen über $GF(q)$ mit Determinante ungleich 0 die Gleichverteilung gegeben.

(a) Ist die Blockchiffre perfekt sicher?

(b) Ändert sich daran etwas, wenn man sowohl im Klar- als auch im Chiffretextraum die 0 entfernt?