Dozent: Prof. Dr. Johannes Blömer
Tutoren: Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
Ausgabedatum: 16.10.2015 **Abgabe:** Mo. 26.10.2015 bis 14:45 Uhr

Einführung in Kryptographie

WS 2015/2016

Heimübungszettel 0

Durch Lösen von Aufgaben dieses Zettels können keine Punkte für das Bonussystem erzielt werden, fristgerecht abgegebene Zettel werden jedoch korrigiert.

AUFGABE 1:

a) Berechnen Sie die folgenden Werte von Hand:

(i) $4321 \bmod 42$

(ii) $-4321 \bmod 42$

(iii) $63^{10} \bmod 65$

b) Benutzen Sie den erweiterten Euklidischen Algorithmus, um $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(186, 35) = 186x + 35y$ bestimmen. Geben Sie dabei alle Zwischenschritte des Algorithmus an.

c) Besitzen die Elemente 7 und 9 ein multiplikativ Inverses in $\mathbb{Z}_{15}$? Berechnen Sie jeweils das Inverse für den Fall, dass es existiert.

AUFGABE 2:

Gegeben sei die Matrix

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 0 \end{pmatrix}.$$

a) Besitzt A ein Inverses in $\mathbb{Z}_{26}^{3\times 3}$?

b) Besitzt A ein Inverses in $\mathbb{Z}_{30}^{3\times 3}$?

c) Berechnen Sie die Inversen gegebenenfalls mit der Cramerschen Regel.

AUFGABE 3:

Sei S ein diskreter Wahrscheinlichkeitsraum mit Wahrscheinlichkeitsmaß $\Pr : \mathcal{P}(S) \to \mathbb{R}$. Wir definieren: Zwei Ereignisse $A, B \subseteq S$ mit $\Pr(A) > 0$ und $\Pr(B) > 0$ heißen unabhängig, wenn $\Pr(A \cap B) = \Pr(A) \cdot \Pr(B)$. Beweisen Sie die folgenden Aussagen für den Fall, dass die auftretenden bedingten Wahrscheinlichkeiten definiert sind.

a) Die Ereignisse $A, B \subseteq S$ sind genau dann unabhängig, wenn $\Pr(A \mid B) = \Pr(A)$ und $\Pr(B \mid A) = \Pr(B)$ gilt.

b) Für alle $A, B \subseteq S$ mit gilt:

$$\Pr(B) \cdot \Pr(A|\, B) = \Pr(A) \cdot \Pr(B|\, A)\,.$$

c) Für alle $A \subseteq S$ und alle disjunkten Zerlegungen $S = B_1 \cup B_2 \cup \ldots \cup B_n$ mit $B_i \cap B_j = \emptyset$ für $i \neq j$ gilt:

$$\Pr(A) = \sum_{i=1}^{n} \Pr(A|\, B_i) \cdot \Pr(B_i)\,.$$

d) Für alle $A_1, A_2, \ldots, A_n \subseteq S$ gilt:

$$\Pr(A_1 \cap A_2 \cap \ldots \cap A_n) = \Pr(A_1) \cdot \prod_{i=2}^{n} \Pr(A_i|\, A_1 \cap \ldots \cap A_{i-1})\,.$$

AUFGABE 4:
Gegeben sei der Wahrscheinlichkeitsraum $S = \{0, 1, \ldots, 25\}$ und die Gleichverteilung Pr auf S. Sei A das Ereignis "$x \in S$ mit $\mathrm{ggT}(x, 26) = 1$", sei B das Ereignis "$x \in S$ ist eine Primzahl" und sei C das Ereignis "$x \in S$ ist ≥ 13".

a) Modellieren Sie A, B, C als Teilmengen von S.

b) Bestimmen Sie die bedingten Wahrscheinlichkeiten $\Pr(A|\, B)$, $\Pr(B|\, A)$, $\Pr(A|\, C)$, $\Pr(C|\, A)$, $\Pr(B|\, C)$ und $\Pr(C|\, B)$.

c) Zeigen Sie, dass A und B nicht unabhängig sind.

d) Zeigen Sie, dass B und C nicht unabhängig sind.

e) Zeigen Sie, dass A und C unabhängig sind.

Hinweis: Bearbeiten Sie zuerst Aufgabe 3 auf diesem Übungsblatt.