Prof. Dr. M. Kreuzer
P. Ackermann

Abgabe: 18.04.2005, 10h

# Kryptografie
## Übungsblatt 1

**Aufgabe 1:**
Von der nachstehenden, in Geheimschrift übermittelten Nachricht sind die letzten 10 Zahlen verlorengegangen. Wie lauten sie? Welches kryptographische System wurde benutzt?

10, 4, 13, 13, 12, 4, 8, 20, 1, 16, 14, 15, 12, 20, 7, 12, 2, 12, 20, 4, 12, 15, 17, 4, 19, 1, 8, 20, 1, 19, 8, 20, 18, 2, 4, 19, 2, 14, 2, 15, 4, 14, 12, 15, 6, 16, 13, 2, 15, 1, 5, 8, 13, 10, 4, 8, 4, 13, 12, 4, 14, 4, 18, 2, 12, 1, 4, 15, 12, 1, 8, 19, 1, 12, 4, 14, 18, 2, 12, 12, 17, 20, 16, 19, 2, 14, 13, 12, 15, 10, 2, 4, 6, 8, 13, 1, 4, 8, 15, 16, 20, 1, 19, 4, 10, 4, 13, 13, 12, 4

**Aufgabe 2:**
Sei $N \geq 2, \mathcal{P} = \mathcal{C} = \{0, 1, \ldots, N-1\}, a, b \in \mathcal{P}$. Weiter sei die Abbildung $f : \mathcal{P} \to \mathcal{C}$ definiert durch $f(x) = ax + b \bmod N$.

a) Zeigen Sie, dass $f$ genau dann eine Chiffrier-Abbildung ist, wenn $\mathrm{ggT}(a, N) = 1$. Wie viele verschiedene Chiffrierabbildungen dieser Art gibt es?

b) Sei $N = 26, a = 5, b = 17$. Dechriffieren Sie

$$1, 17, 11, 3, 17, 12$$

Dabei stehe im Klartext 0 für A, 1 für B, ....

**Aufgabe 3:**

a) Schreiben Sie ein Programm `Kasiski(...)` (z.B. in CoCoA), das als Eingabe eine Zeichenkette („String“) erwartet und als Ausgabe eine Liste von Zahlen errechnet, die aus den Distanzen mindestens zweimal vorkommender Zeichenketten der Länge $\geq 3$ besteht. Die Distanz sei hierbei definiert als die Differenz der Positionen der Anfangsbuchstaben.

b) Schreiben Sie ein weiteres Programm `Divisors(...)`, das die soeben berechnete Liste nimmt und eine Liste von Kandidaten für die Schlüssellänge beim Kasiski–Test bestimmt. Erklären Sie, wie Sie den Fall von „Ausreißern“ handhaben.

c) Wenden Sie die beiden Programme auf den Text in `Aufgabe3.txt` an.

**Allgemeines:**
Die Programmieraufgaben bitte sowohl ausdrucken als auch per E-Mail and den Übungsleiter senden.