

## Übungsblatt 8

### Aufgabe 28 (schriftlich, 10 Punkte)

- a) Bestimmen Sie in Abhängigkeit von der Redundanz  $R_L$  der Klartextsprache und der Größe  $m$  des Alphabets  $A$  näherungsweise die Eindeutigkeitsdistanz
- einer einfachen Substitutionschiffre,
  - einer Hill-Chiffre mit Blocklänge  $l$ ,
  - einer Blocktransposition mit Blocklänge  $l$  und
  - einer Blockchiffre, in der jede Bijektion auf  $M = A^l$  durch (genau) einen Schlüssel  $k \in K$  realisiert wird.

**Hinweis:** Benützen Sie zur Abschätzung von  $n!$  die Stirling-Formel  $n! \approx \sqrt{2\pi n}(n/e)^n$ .

- b) Geben Sie für jede dieser Chiffren einen möglichst langen Kryptotext  $y$  mit  $\|K(y)\| > 1$  an, falls Deutsch als Klartextsprache benutzt wird. (Die Blocklänge  $l$  können Sie beliebig zwischen 2 und 5 wählen).

### Aufgabe 29

- a) Definieren Sie formal, wann zwei Kryptosysteme als gleich (besser: äquivalent) anzusehen sind. Betrachten Sie auch den Fall, dass Wahrscheinlichkeitsverteilungen auf den Schlüsselräumen gegeben sind.
- b) Zeigen Sie, dass die affine Chiffre idempotent ist.

### Aufgabe 30

Überlegen Sie, wie sich ein durch ein SPN verschlüsselter Kryptotext  $y = E_{f, \pi_S, \pi_P}(K, x)$  wieder zu  $x$  entschlüsseln lässt.

### Aufgabe 31

Seien  $X_1, X_2, X_3$  unabhängige Zufallsvariablen mit Wertebereich  $W(X_i) = \{0, 1\}$  und bias  $\varepsilon(X_i)$  für  $i = 1, 2, 3$ . Zeigen Sie, dass die Zufallsvariablen  $X_1 \oplus X_2$  und  $X_2 \oplus X_3$  genau dann unabhängig sind, wenn  $\varepsilon(X_1) = 0$  oder  $\varepsilon(X_3) = 0$  oder  $\varepsilon(X_2) = \pm 1/2$  ist.