Übungen zur Kryptologie 1 Wintersemester 05/06
Johannes Köbler/Olaf Beyersdorff

Übungsblatt 7

Aufgabe 25 (mündlich)

Ein Kryptosystem ist genau dann unter allen Klartextverteilungen absolut sicher, wenn es unter jeder Klartextverteilung p mit $p(x) \in \{0, 1/2\}$ für alle $x \in M$ absolut sicher ist.

Aufgabe 26 (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 kann beliebig zwischen 2 und 5 gewählt werden).

Aufgabe 27 (mündlich)

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 28 (mündlich)

Seien S_1 und S_2 Vigenère-Chiffren mit fester Schlüsselwortlänge d_1 bzw. d_2.

a) Zeigen Sie: Ist d_1 ein Teiler von d_2, so gilt $S_1 \times S_2 = S_2$.

b) Lässt sich Teilaufgabe a) verallgemeinern zu $S_1 \times S_2 = S_3$, wobei S_3 die Vigenère-Chiffre mit Schlüsselwortlänge $d = \mathrm{kgV}(d_1, d_2)$ ist?

Aufgabe 29 (mündlich)

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