Übungen zur Kryptologie 1 Wintersemester 07/08

Johannes Köbler/Sebastian Kuhnert

Übungsblatt 7

Aufgabe 28 (schriftlich, 10 Punkte)

Zeigen Sie, dass ein Kryptosystem unter jeder Klartextverteilung absolut sicher ist, falls kein Gegner mit einem Vorteil $\alpha(G, V) > 0$ existiert.
Hinweis: Zeigen Sie, dass in einem nicht absolut sicheren Kryptosystem Klartexte x_0, x_1 und ein Kryptotext y existieren mit $p(x_0|y) < p(x_0)$, wobei für die Klartextverteilung $p(x_0) = p(x_1) = 1/2$ gilt.

Aufgabe 29 (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 30 (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 31 (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.

Aufgabe 32 (mündlich)

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.

Aufgabe 33 (mündlich)

Bestimmen Sie für die durch folgende Permutation $\pi_{S'}$ definierte S-Box S' sämtliche Werte $L(a, b)$ für $a, b \in \{0, 1\}^4$.

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_{S'}(z)$	8	4	2	1	C	6	3	D	A	5	E	7	F	B	9	0