Übungsblatt 6

Aufgabe 25 ***mündlich***

(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 26 ***mündlich***

Sei $S = (M, C, E, D, K)$ ein Kryptosystem und bezeichne $\alpha_{\max}$ den maximalen Vorteil, den ein Gegner (mit unbeschränkten Rechenressourcen) erzielen kann. Zeigen Sie:

(a) Wenn $\|K\| < \|M\|$ ist, dann ist $\alpha_{\max} > 0$.

(b) Wenn $\|K\|\,(\|K\| - 1) < \|M\| - 1$ ist, dann ist $\alpha_{\max} = 1/2$.

(c) Über welche Rechenressourcen muss ein optimaler Gegner in Teilaufgabe (b) höchstens verfügen, wenn die Verschlüsselungsfunktion E effizient berechenbar ist?

Aufgabe 27 Zeigen Sie: ***mündlich***

(a) In einem absolut sicheren Kryptosystem hängt die Kryptotextverteilung nicht von der Verteilung der Klartexte ab.

(b) 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.

(c) Ein Kryptosystem ist absolut sicher, falls kein Gegner mit einem Vorteil $\alpha(G, V) > 0$ existiert.

Aufgabe 28 ***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 29 ***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 ist $S_1 \times S_2 = S_2$.

(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 30 ***mündlich***

Seien H_1, H_2 und H_3 Hill-Chiffren mit Blocklängen l_1, l_2 und l_3.

(a) Zeigen Sie, dass $H_1 \times H_1 = H_1$ ist.

(b) Was muss für l_1, l_2 und l_3 gelten, damit $H_1 \times H_2 = H_3$ ist?
Hierbei bezeichne $H_1 \times H_2$ (abweichend vom Skript) die Chiffre mit Blocklänge $\mathrm{kgV}(l_1, l_2)$, die erst H_1 und dann H_2 blockweise anwendet.

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***

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

Aufgabe 33 ***10 Punkte***

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.