# Übungsblatt 6

***Abgabe für die mündlichen Aufgaben bis 02. 06. 2020 und für die schriftliche Aufgabe bis 09. 06. 2020***

**Aufgabe 32** ***mündlich***

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

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

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

(c) Wie groß ist der Zeitufwand für den Gegner in Teilaufgabe (b) in Abhängigkeit von $\|M\|$, $\|K\|$ und dem Aufwand $v$ für eine Klartextverschlüsselung?

**Aufgabe 33** ***mündlich***

Seien $KS_i = (M_i, C_i, K_i, D_i, E_i, S_i)$ $(i \in \{1,2\})$ Kryptosysteme. Wir sagen, zwei Abbildungen $f: M_1 \to M_2$ und $g: C_2 \to C_1$ **reduzieren** einen Schlüssel $k_1$ in $KS_1$ auf einen Schlüssel $k_2$ in $KS_2$, falls für alle $x \in M_1$ gilt: $E_1(k_1, x) = g(E_2(k_2, f(x)))$.

(a) Definieren Sie auf der Grundlage dieser Reduktion zwischen einzelnen Schlüsseln die Äquivalenz der beiden Kryptosysteme $KS_1$ und $KS_2$.

*Hinweis:* Beziehen Sie die Schlüsselgeneratoren $S_1$ und $S_2$ erst in einem zweiten Schritt in Ihre Definition mit ein und verlangen Sie nicht $\|K_1\| = \|K_2\|$.

(b) Zeigen Sie, dass die affine Chiffre $A = (\mathbb{Z}_m, \mathbb{Z}_m, K, E, D, S)$ ($S$ gleichverteilt auf $K = \mathbb{Z}_m^* \times \mathbb{Z}_m$) idempotent ist (d.h. die Produktchiffre $A \times A$ ist äquivalent zu $A$).

**Aufgabe 34** ***mündlich***

Seien $V_1$ und $V_2$ Vigenère-Chiffren über demselben Alphabet $A$ mit fester Schlüsselwortlänge $d_1$ bzw. $d_2$.

(a) Zeigen Sie: Ist $d_1$ ein Teiler von $d_2$, so ist $V_1 \times V_2$ äquivalent zu $V_2$.

(b) Lässt sich Teilaufgabe (a) verallgemeinern zu $V_1 \times V_2 = V_3$, wobei $V_3$ die Vigenère-Chiffre mit Schlüsselwortlänge $d = \mathrm{kgV}(d_1, d_2)$ ist?

(c) Zeigen Sie, dass die Vigenère-Chiffre mit Schlüsselraum $K = A^*$ idempotent ist.

**Aufgabe 35** ***mündlich***

Sei $A$ ein Alphabet und seien $H_1, H_2$ und $H_3$ Hill-Chiffren über $A$ mit Blocklängen $\ell_1, \ell_2$ und $\ell_3$.

(a) Zeigen Sie, dass die Chiffren $H_i$ idempotent sind.

(b) Die Produktchiffre $H_1 \times H_2$ der beiden Hill-Chiffren $H_1$ und $H_2$ lässt sich nach unserer bisherigen Definition nur im Fall $\ell_1 = \ell_2$ bilden. Verallgemeinern Sie die Definition der Produktchiffre $H = H_1 \times H_2$ auf beliebige Blocklängen $\ell_1, \ell_2 \geq 1$.

*Hinweis:* $H$ hat die Blocklänge $\ell = \mathrm{kgV}(\ell_1, \ell_2)$.

(c) Für welche Blocklängen $\ell_1, \ell_2, \ell_3 \geq 1$ gilt $H_1 \times H_2 = H_3$?

**Aufgabe 36** ***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 37** ***mündlich***

Sei $\sigma_S: \{0,1\}^l \to \{0,1\}^{l'}$ eine S-Box und für $(a,b) \in \{0,1\}^l \times \{0,1\}^{l'}$ sei $L(a,b)$ die Anzahl der Paare $(x,y) \in \left\{(x, \sigma_S(x)) \,\middle|\, x \in \{0,1\}^l\right\}$, für die $\bigoplus_{i=1}^{l} a_i x_i = \bigoplus_{j=1}^{l'} b_j y_j$ ist. Zeigen Sie:

(a) $L(0^l, 0^{l'}) = 2^l$,

(b) $L(a, 0^{l'}) = 2^{l-1}$ für alle $a \in \{0,1\}^l - \{0^l\}$,

(c) $\sum_{a \in \{0,1\}^l} L(a,b) = 2^{2l-1} \pm 2^{l-1}$ für alle $b \in \{0,1\}^{l'}$,

(d) $\sum_{\substack{a \in \{0,1\}^l \\ b \in \{0,1\}^{l'}}} L(a,b) = \begin{cases} 2^{2l+l'-1} + 2^{l+l'-1} & \sigma_S(0^l) = 0^{l'}, \\ 2^{2l+l'-1} & \text{sonst.} \end{cases}$

**Aufgabe 38** ***mündlich, 10 Punkte***

Zeigen oder widerlegen Sie folgende Aussagen:

(a) Ist ein Kryptosystem absolut sicher, so gilt $p(y_1) = p(y_2)$ für alle $y_1, y_2 \in C$. ***mündlich***

(b) In jedem Kryptosystem gilt $\mathcal{H}(S|Y) \geq \mathcal{H}(X|Y)$. ***mündlich***

(c) In einem absolut sicheren Kryptosystem gilt $\mathcal{H}(X) \leq \mathcal{H}(S)$. ***mündlich***

(d) Ein Kryptosystem ist genau dann absolut sicher, falls kein Gegner mit einem Vorteil $\alpha_G > 0$ existiert. ***10 Punkte***