Übungsblatt 6

Abgabe der schriftlichen Lösungen am 7. 12. 2017 bis 13.10 Uhr

Aufgabe 28 ***mündlich***

Sei (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 29 ***mündlich***

Seien $S_i = (M_i, C_i, K_i, D_i, E_i)$ $(i \in \{1, 2\})$ Kryptosysteme und $f\colon M_1 \to M_2$ und $g\colon C_1 \to C_2$ bijektive Abbildungen. Wir nennen zwei Schlüssel $k_1 \in K_1$ und $k_2 \in K_2$ (f, g)**-äquivalent**, falls für alle $x \in M_1$ gilt: $g(E_1(k_1, x)) = E_2(k_2, f(x))$.

(a) Definieren Sie formal, wann zwei Kryptosysteme S_1 und S_2 äquivalent sind (verlangen Sie nicht $\|K_1\| = \|K_2\|$). Betrachten Sie auch den Fall, dass Schlüsselgeneratoren Z_1 und Z_2 für S_1 und S_2 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 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?

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

Aufgabe 31 ***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 32 ***mündlich***

Sei E die Chiffrierfunktion einer (binären) Blockchiffre S mit Blocklänge l und Schlüsselraum $\{0,1\}^k$. Wir betrachten einen Angriff bei *bekanntem Klartext*, d. h. es steht eine ausreichende Zahl von Klartext-Kryptotext-Paaren $(x_i, y_i), i = 1, \ldots, t$, zur Verfügung, die alle mit demselben unbekannten Schlüssel K generiert wurden.

(a) Bestimmen Sie heuristisch die erwartete Anzahl von Schlüsseln K, die zu allen Paaren (x_i, y_i) »passen«, d. h. es gilt $E_K(x_i) = y_i$ für $i = 1, \ldots, t$.

Hinweis: Gehen Sie davon aus, dass für einen zufällig gewählten Schlüssel K die Wahrscheinlichkeit $\Pr[E_K(x) = y]$, dass K einen gegebenen Klartext x durch den Kryptotext y chiffriert, gleich 2^{-l} ist (selbst dann, wenn bereits bekannt ist, dass K gewisse Klartexte $x_i \neq x$ durch gewisse Kryptotexte y_i chiffriert).

(b) Wie lässt sich im Fall $t \geq k/l$ der benutzte Schlüssel K mittels $t2^k$ Verschlüsselungen bestimmen?

(c) Um die Sicherheit zu erhöhen, wird nun das Kryptosystem $S \times S$ verwendet, d. h. die Schlüssellänge verdoppelt sich auf $2k$. Zeigen Sie, dass sich dadurch die benötigte Anzahl t an Klartext-Kryptotext-Paaren (x_i, y_i) ebenfalls (auf $2k/l$) verdoppelt.

(d) Wie lässt sich im Fall $t \geq 2k/l$ der benutzte Schlüssel (K, K') unter Verwendung eines Speichers der Größe $(lt + k)2^k$ mittels $t2^{k+1}$ Ver- und Entschlüsselungen bestimmen?

(e) Überlegen Sie, wie sich der Platzbedarf in (d) auf Kosten der Rechenzeit reduzieren lässt. Suchen Sie nach einer möglichst allgemeinen Beziehung für diesen so genannten *Time-Memory-Tradeoff*.

Aufgabe 33 ***5 Punkte, rechenintensiv***

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

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

Hinweis: $L(a, b) := \left\|\left\{x \in \{0,1\}^4 \;\middle|\; \sum_{i=1}^4 a_i x_i \mod 2 = \sum_{i=1}^4 b_i y_i \mod 2, y = \pi_{S'}(x)\right\}\right\|$, d.h. $L(a, b)$ bezeichnet die Anzahl der Paare $(x, \pi_{S'}(x))$, in denen das XOR der durch a ausgewählten Bits der Eingabe gleich dem XOR der durch b ausgewählten Bits der Ausgabe ist.

Rückseite beachten!

Aufgabe 34 ***5 Punkte***

Seien X_1, X_2, X_3 unabhängige Zufallsvariablen mit Wertebereich $W(X_i) = \{0, 1\}$ und Bias $\varepsilon_i = \varepsilon(X_i)$ 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 $\varepsilon_1 = 0$ oder $\varepsilon_3 = 0$ oder $\varepsilon_2 = \pm 1/2$ ist.

Hinweis: Der Bias $\varepsilon(X)$ ist definiert als: $\varepsilon(X) := \Pr[X = 0] - 1/2$.