Übungsblatt 6

Abgabe der schriftlichen Lösungen bis 09.06.2022, 24 Uhr

Aufgabe 31 ***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 $\mathcal{H}(S|\mathcal{Y}) \geq \mathcal{H}(\mathcal{X}|\mathcal{Y})$. ***mündlich***

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

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

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 Zeitaufwand für den Gegner G in Teilaufgabe (b) in Abhängigkeit von $|M|$, $|K|$ und dem Aufwand v für eine Ver- bzw. Entschlüsselung?

Aufgabe 33 ***mündlich***

Seien $KS = (M, C, K, D, E)$ und $KS' = (M, C, K', D', E')$ Kryptosysteme. Wir sagen, eine Abbildung $f: K \to K'$ **reduziert** KS auf KS', falls $E(k, x) = E'(f(k), x)$ für alle $(k, x) \in K \times M$ gilt.

(a) Definieren Sie auf der Grundlage dieser Reduktion die Äquivalenz der beiden Kryptosysteme KS und KS'.

Hinweis: Lassen Sie zu, dass $|K| \neq |K'|$ ist.

(b) Erweitern Sie Ihre Definition auf Kryptosysteme $KS = (M, C, K, D, E, \mathcal{S})$ und $KS' = (M, C, K', D', E', \mathcal{S}')$ mit einem Schlüsselgenerator.

(c) Zeigen Sie, dass die affine Chiffre $KS = (\mathbb{Z}_m, \mathbb{Z}_m, K, E, D, \mathcal{S})$ mit gleichverteiltem Schlüssel idempotent ist (d.h. die Produktchiffre $KS \times KS$ ist äquivalent zu KS).

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, dass $V_1 \times V_2$ äquivalent zu V_2 ist, falls d_1 ein Teiler von d_2 ist.

(b) Lässt sich Teilaufgabe (a) zu $V_1 \times V_2 = V_3$ verallgemeinern, wobei V_3 die Vigenère-Chiffre mit Schlüsselwortlänge $d_3 = \mathrm{kgV}(d_1, d_2)$ ist?

(c) Zeigen Sie, dass die Vigenère-Chiffre V mit variabler Schlüssellänge (d.h. $K = A^*$) idempotent ist.

Aufgabe 35 ***mündlich***

Sei A ein Alphabet und seien H_1, H_2 und H_3 Hill-Chiffren über A mit Blocklängen ℓ_1, ℓ_2 und ℓ_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 $H_1 \times H_2 = H_3$?