Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Kryptologie - WiSe 2022/23
8. November 2022

Übungsblatt 4

Besprechung der mündlichen Aufgaben am 17. 11. 2022
Abgabe der schriftlichen Lösungen bis 22. 11. 2022, 23:59 Uhr

Aufgabe 19 ***mündlich***

Sei $h\colon \{0,1\}^{m+t} \to \{0,1\}^m$ eine kollisionsresistente Kompressionsfunktion. Wie in der Vorlesung gezeigt, kann h zu einer kollisionsresistenten Hashfunktion $\hat{h}\colon \{0,1\}^* \to \{0,1\}^m$ erweitert werden, sofern hierzu ein öffentlich bekannter Initialisierungsvektor $IV \in \{0,1\}^m$ und eine suffixfreie Preprocessing-Funktion y verwendet werden (wobei wir auf die optionale Ausgabetransformation verzichten).

Für die Preprocessing-Funktion wird meist eine Funktion der Bauart $y(x) = x\,pad(x)$ verwendet, wobei $pad\colon \{0,1\}^* \to \{0,1\}^*$ eine so genannte Paddingfunktion mit $|x| + |pad(x)| \equiv_t 0$ ist. Um nun einen MAC zu konstruieren, könnte man $K = \{0,1\}^m$ als Schlüsselraum wählen und bei der Berechnung von $\hat{h}(x)$ anstelle von IV den geheimen Schlüssel k benutzen, um $h_k(x)$ zu erhalten.

Zeigen Sie, dass der so konstruierte MAC nicht berechnungsresistent ist, indem Sie einen Substitutionsangriff durchführen.

Aufgabe 20 ***mündlich***

Berechnen Sie α und β für den MAC mit nebenstehender Authentikationsmatrix. Die Wahrscheinlichkeitsverteilung auf der Textmenge $X = \{a,b,c,d\}$ sei

$$p(a) = p(d) = 1/6,\ p(b) = p(c) = 1/3$$

und die Wahrscheinlichkeitsverteilung auf dem Schlüsselraum K sei

$$p(k_1) = p(k_6) = 1/4,\ p(k_2) = p(k_3) = p(k_4) = p(k_5) = 1/8.$$

	a	b	c	d
k_1	1	1	2	3
k_2	1	2	3	1
k_3	2	1	3	1
k_4	2	3	1	2
k_5	3	2	1	3
k_6	3	3	2	1

Geben Sie auch die optimalen Impersonations- und Substitutionsstrategien an.

Aufgabe 21 ***mündlich***

(a) Geben Sie einen MAC an, bei dem $\alpha > \beta$ gilt.

(b) Zeigen Sie, dass für jeden (n,m,l)-MAC gilt: $\beta = 1/m \Rightarrow \alpha = 1/m$.

Aufgabe 22 ***mündlich***

Sei eine Textmenge X und eine Menge Y von MAC-Werten mit $\|Y\| = m$ vorgegeben. Charakterisieren Sie die MACs mit dem optimalen Wert $\alpha = 1/m$ und minimaler Schlüsselmenge K (bei geeigneter Wahl der Wahrscheinlichkeitsverteilung auf K).

Aufgabe 23 ***mündlich***

Zeigen Sie, dass die in der Vorlesung hergeleitete Entropieschranke für die Impersonationswahrscheinlichkeit α »scharf« ist.

Hinweis: Betrachten Sie einen beliebigen 2-universalen MAC.

Aufgabe 24 ***5 Punkte***

Angenommen, Sie wollen Nachrichten über dem 26-stelligen Alphabet $\{A, \ldots, Z\}$ der Länge 1000 authentisieren. Wie könnte ein entsprechender MAC aussehen, falls die Erfolgswahrscheinlichkeit eines Ressourcen-unbeschränkten Gegners bei Durchführung eines Impersonations- oder Substitutionsangriffs nicht größer als 10^{-4} sein soll?

Aufgabe 25 ***5 Punkte***

Schreiben Sie ein Programm, das für den MAC aus Aufgabe 20 die Entropiewerte $H(\mathcal{K})$ und $H(\mathcal{K}|\mathcal{X}, \mathcal{Y})$ und daraus die in der Vorlesung hergeleitete Schranke $\alpha \geq 2^{H(\mathcal{K}|\mathcal{X},\mathcal{Y})-H(\mathcal{K})}$ berechnet. Vergleichen Sie diese Schranke mit dem tatsächlichen Wert von α. Hierbei stehen $\mathcal{K}, \mathcal{X}$ für unabhängige Zufallsvariablen mit $\forall k \in K : \Pr[\mathcal{K} = k] = p(k)$ und $\forall x \in X : \Pr[\mathcal{X} = x] = p(x)$ und es gilt $\mathcal{Y} = h_{\mathcal{K}}(\mathcal{X})$.