Die Lösung zur Teilaufgabe **7.1 b** wird als Teil der Prüfungsnote **bewertet**! Bitte mit Angabe von Name, Matrikelnummer, Studiengang und Fachsemester bei der Übung am 2. Juli abgeben (oder vorher per E-Mail an `bmoeller@crypto.rub.de`).

Aufgabe 7.1 [PRF als MAC]

Vorbemerkungen

Bisher hatten wir für das Konzept der *Pseudo-Random Function* (PRF) nur Abbildungen betrachtet, bei denen die Definitionsmenge mit der Zielmenge übereinstimmt. Diese Einschränkung ist eigentlich nicht nötig, allgemeiner können wir auch Abbildungen $\{0,1\}^* \to \{0,1\}^\ell$ betrachten.

Sei also $\mathcal{K}$ eine Menge von Schlüsseln, und sei für jedes $K \in \mathcal{K}$ eine Abbildung

$$f_K : \{0,1\}^* \to \{0,1\}^\ell$$

definiert. Das PRF-Angriffsspiel für einen Angreifer $\boldsymbol{B}$ sieht aus wie gewohnt: Der Angreifer hat Zugriff auf ein Orakel, das entweder Werte von f_K für ein zufälliges K bietet (dafür schreiben wir $\boldsymbol{B}^{f_K(\cdot)}$) oder Werte einer gleichverteilt zufälligen Abbildung $f\colon \{0,1\}^* \to \{0,1\}^\ell$ (wir schreiben $\boldsymbol{B}^{f(\cdot)}$). Letzteres heißt, die $f(x)$ für alle $x \in \{0,1\}^*$ sind unabhängig gleichverteilt in $\{0,1\}^\ell$; für diese Verteilung schreiben wir $f \in_\$ \mathrm{Func}(\{0,1\}^*, \{0,1\}^\ell)$. Der Angreifer gibt schließlich ein Bit aus. Sein Erfolg wird gemessen als PRF-Vorteil

$$\mathrm{Adv}^{\mathsf{PRF}}_{f_K,\boldsymbol{B}} = \Pr_{K\in_\$\mathcal{K}}\bigl(\boldsymbol{B}^{f_K(\cdot)} \Rightarrow 1\bigr) - \Pr_{f\in_\$\mathrm{Func}(\{0,1\}^*,\{0,1\}^\ell)}\bigl(\boldsymbol{B}^{f(\cdot)} \Rightarrow 1\bigr).$$

Von *PRF-Sicherheit* der Familie f_K sprechen wir (wie gewohnt) dann, wenn dieser Vorteil für jeden denkbaren Angreifer verschwindend gering bleibt.

Einen *Message Authentication Code* (MAC) haben wir definiert als $(\mathcal{K}_M, MAC, VF)$ mit

- einem *Schlüsselerzeugungsalgorithmus* $\mathcal{K}$ zur Generierung eines K;
- einem *MAC-Erzeugungsalgorithmus,* der zu jedem $m \in \{0,1\}^*$ eine Ausgabe $MAC_K(m) \in \{0,1\}^\ell$ erzeugt;
- und einem *MAC-Überprüfungsalgorithmus,* der zu $m \in \{0,1\}^*$ und $t \in \{0,1\}^\ell$ eine Ausgabe $VF_K(m,t) \in \{\mathsf{true}, \mathsf{false}\}$ erzeugt.

Ein Message Authentication Code soll *korrekt* sein: Zu von $\mathcal{K}$ erzeugtem K und $m \in \{0,1\}^*$ muss stets gelten $VF_K\bigl(m, MAC_K(m)\bigr) = \mathsf{true}$. Außerdem wünschen wir Sicherheit, definiert über ein *MAC-Angriffsspiel* mit Angreifer $\boldsymbol{A}$:

- Der Angreifer hat Orakelzugriff auf $MAC_K(\cdot)$ und auf $VF_K(\cdot,\cdot)$ zu einem zufälligem K;
- dabei sind Anfragen $VF_K(m, tag)$ nicht zulässig, falls *tag* vorher die Antwort auf eine Anfrage $MAC_K(m)$ war;
- der Angreifer gewinnt das Spiel, wenn $VF_K(\cdot,\cdot)$ jemals auf eine zulässige Anfrage die Antwort true gibt.

Der MAC-Vorteil $\mathrm{Adv}^{\mathsf{MAC}}_{(\mathcal{K},MAC,VF),\boldsymbol{A}}$ ist die Wahrscheinlichkeit, dass $\boldsymbol{A}$ in diesem Angriffsspiel gewinnt. Der Message Authentication Code ist *sicher,* wenn dieser Vorteil für jeden denkbaren Angreifer verschwindend gering ist.

Aufgabe

Nun kann man versuchen, Pseudo-Random Functions (die durch effiziente Algorithmen realisiert werden können) als MAC einzusetzen:

- $\mathcal{K}$ als Schlüsselerzeugungsalgorithmus wählt ein gleichverteilt zufälliges Element der Menge $\mathcal{K}$;
- $MAC_K(m)$ gibt den Wert $f_K(m)$ aus;
- $VF_K(m, tag)$ berechnet zunächst $t = MAC_K(m)$ und gibt dann true aus, falls $tag = t$; false sonst.

Zeigen Sie dafür:

a. Mit dieser Definition ist $(\mathcal{K}, MAC, VF)$ als MAC korrekt.

b. $(\mathcal{K}, MAC, VF)$ ist als MAC sicher, falls die Familie der f_K PRF-sicher ist.

Hinweise zu Aufgabe 7.1 b

Nehmen Sie einen MAC-Angreifer $\boldsymbol{A}$ auf $(\mathcal{K}, MAC, VF)$ an, der höchstens q Anfragen an das Orakel für $VF_K(\cdot,\cdot)$ stellt. Beschreiben Sie auf Basis von $\boldsymbol{A}$ einen PRF-Angreifer $\boldsymbol{B}$, der $\boldsymbol{A}$ verwendet und mit Hilfe seines eigenen Orakels ($f_K(\cdot)$ oder $f(\cdot)$) das MAC-Angriffsspiel für $\boldsymbol{A}$ nachbildet und der schließlich den Wert 1 ausgibt, falls $\boldsymbol{A}$ im nachgebildeten Angriffsspiel gewinnt; 0 sonst:

- Was muss $\boldsymbol{B}$ tun, wenn $\boldsymbol{A}$ eine Anfrage m an sein erwartetes Orakel für $MAC_K(\cdot)$ stellt?
- Was muss $\boldsymbol{B}$ tun, wenn $\boldsymbol{A}$ eine Anfrage (m, tag) an sein erwartetes Orakel für $VF_K(\cdot,\cdot)$ stellt?

Folgern Sie nun

$$\mathrm{Adv}^{\mathsf{MAC}}_{(\mathcal{K},MAC,VF),\boldsymbol{A}} \;\leq\; \mathrm{Adv}^{\mathsf{PRF}}_{f_K,\boldsymbol{B}} + \frac{q}{2^\ell},$$

indem Sie einerseits

$$\Pr_{K\in_\$\mathcal{K}}\bigl(\boldsymbol{B}^{f_K(\cdot)} \Rightarrow 1\bigr)$$

betrachten und andererseits

$$\Pr_{f\in_\$\mathrm{Func}(\{0,1\}^*,\{0,1\}^\ell)}\bigl(\boldsymbol{B}^{f(\cdot)} \Rightarrow 1\bigr).$$

Die Ungleichung bietet die gewünschte Sicherheitsaussage.