Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Florian Giesen

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 1

WS 2010/11

Blatt 7 / 24./26. Januar 2011

Im Korollar zur Sicherheit des HMAC (Folie 137) benötigt man folgende drei Annahmen.

i) Die Kollisionsresistenz der Kompressionsfunktion (Gen', h).

ii) Die Sicherheit des aus Π abgeleiteten MACs Π_h fester Länge (siehe Folie 131).

iii) Die Pseudozufälligkeit des aus Π abgeleiteten Generators G (siehe Folie 137).

Wir wollen in der folgenden Aufgabe zeigen, dass Eigenschaft iii) im Allgemeinen nicht aus der Kollisionsresistenz von Π folgt.

AUFGABE 1. HMAC.
Konstruieren Sie eine kollisionsresistente Hashfunktion $\Pi = (\mathsf{Gen}, h)$ mit $h_s : \{0,1\}^{2\ell} \to \{0,1\}^{\ell}$, so dass die Funktion

$$\begin{aligned} G : \{0,1\}^{\ell} &\to \{0,1\}^{2\ell} \\ k &\mapsto h_s(\mathsf{IV}||k \oplus \mathsf{opad})||h_s(\mathsf{IV}||k \oplus \mathsf{ipad}) \end{aligned}$$

kein Pseudozufallsgenerator ist. Hierbei sind $\mathsf{IV}, \mathsf{opad}, \mathsf{ipad} \in \{0,1\}^{\ell}$ feste Konstanten mit $\mathsf{opad} \neq \mathsf{ipad}$. Gehen Sie hierzu wie folgt vor.

a) Es sei $\widetilde{\Pi} = (\widetilde{\mathsf{Gen}}, g)$ mit $g_s : \{0,1\}^{2\ell} \to \{0,1\}^{\ell-1}$ eine kollisionsresistente Hashfunktion. Zeigen Sie, dass dann auch $\Pi = (\mathsf{Gen}, h)$ mit $h_s : \{0,1\}^{2\ell} \to \{0,1\}^{\ell}$ und $h_s(x) := (g_s(x)||0)$ kollisionsresistent ist.

b) Zeigen Sie, dass G instantiiert mit Π aus Teil a) *kein* Pseudozufallsgenerator ist, indem Sie konkret einen Unterscheider angeben.

AUFGABE 2. Encrypt and Authenticate.
Es sei $\Pi_E = (\mathsf{Gen}_E, \mathsf{Enc}, \mathsf{Dec})$ ein CPA-sicheres Verschlüsselungsverfahren und $\Pi_M = (\mathsf{Gen}_M, \mathsf{Mac}, \mathsf{Vrfy})$ ein MAC mit eindeutigen Tags (siehe Folie 140). Zeigen Sie, dass „Encrypt-and-Authenticate“ hierfür *niemals* ein sicheres Nachrichtenübermittlungsverfahren (Folie 145) sein kann.

Hinweis: Betrachten Sie $c = (\mathsf{Enc}_{k_1}(m), \mathsf{Mac}_{k_2}(m))$ und zeigen Sie, dass das Verfahren *nicht* CPA-sicher ist.

AUFGABE 3. CCA vs. authentisierte Kommunikation.
Konstruieren Sie ein Verschlüsselungsverfahren $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, welches CCA-sicher ist, aber *keine* authentisierte Kommunikation (siehe Folie 145) bietet.

Hinweis: Gehen Sie von einem CCA-sicheren Verfahren aus, und fügen Sie einen „künstlichen“ Chiffretext für einen ausgezeichneten Klartext hinzu, welcher aber gar nicht von Enc ausgegeben wird.