Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Stefan Hoffmann, Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptographie

WS 2013/14

Blatt 7 / 25./26. November 2013

AUFGABE 1:

Sei (Gen, H) eine kollisionsresistente Hashfunktion. Betrachten Sie nun die Hashfunktion $(\mathsf{Gen}, \hat{H})$ mit $\hat{H}_s(x) := (s, H_s(x))$.

Ist die neue Hashfunktion kollisionsresistent? Falls ja, geben Sie eine Reduktion an, die aus einer Kollision in $\hat{H}$ eine Kollision in H bestimmt. Falls nein, geben Sie einen Angreifer an, der eine Kollision in $\hat{H}$ berechnet.

AUFGABE 2 (5 Punkte):

Sei $\Pi' = (\mathsf{Gen}', \mathsf{Mac}', \mathsf{Vrfy}')$ ein sicherer MAC für Nachrichten der festen Länge n. Betrachten Sie den folgenden MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ für Nachrichten der festen Länge $2n - 2$:

$\mathsf{Gen}(1^n)$: Gib $k \leftarrow \mathsf{Gen}'(1^n)$ zurück.

$\mathsf{Mac}_k(m)$: Für $m = (m_0, m_1)$ mit $m_i \in \{0,1\}^{n-1}$ gib zurück:

$$t := (t_0, t_1) := (\mathsf{Mac}'_k(m_0, 0), \mathsf{Mac}'_k(m_1, 1))$$

(a) Geben Sie eine korrekte Vrfy-Funktion an.

(b) Zeigen Sie, dass Π nicht sicher ist.

AUFGABE 3:

Betrachten Sie folgende Modifikationen des CBC-MAC aus der Vorlesung (siehe Folie 117).

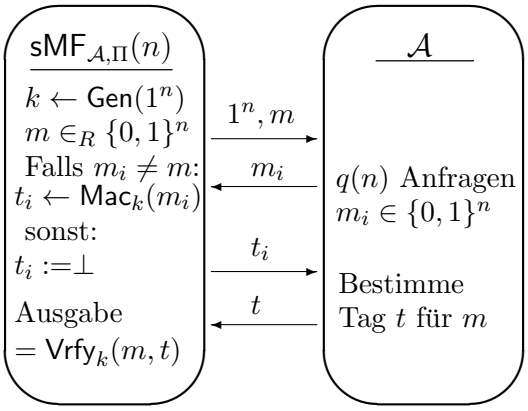
(a) Beweisen Sie, dass der CBC-MAC aus der Vorlesung nicht sicher ist, wenn wir Nachrichten mit *variabler* Länge zulassen.

(b) Anstelle eines fixen $t_0 := 0^n$ wählen wir nun zufälliges $t_0 \in_R \{0,1\}^n$ und geben dieses am Ende zusätzlich mit aus, d.h. der Tag hat die Form $t := (t_0, t)$. Zeigen Sie, dass diese Konstruktion unsicher ist.

AUFGABE 4:

Wir definieren einen neuen Sicherheitsbegriff eines *schwach sicheren* MACs. Im zugehörigen Sicherheitsspiel sMF darf der Angreifer $\mathcal{A}$ im Vergleich zum Sicherheitsspiel $\mathsf{Mac\text{-}Forge}$ die zum gefälschten Tag gehörige Nachricht nicht selbst wählen. Stattdessen wird eine uniform gewählte Nachricht m zu Beginn vorgegeben.

Das Sicherheitsspiel sMF:



Die Sicherheitsdefinition für einen MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$:

> Π heißt *schwach sicher*, falls für alle ppt-Angr. $\mathcal{A}$: $\mathsf{Ws}[\mathsf{sMF}_{\mathcal{A},\Pi}(n) = 1] \leq \mathsf{negl}(n)$.

Zeigen Sie mit Hilfe einer Reduktion, dass jeder *sichere* MAC Π für Nachrichten $m \in \{0,1\}^n$ auch *schwach sicher* ist.