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

Hausübungen zur Vorlesung

Kryptographie I

WS 2012/13

Blatt 6 / 18. Dezember 2012

Abgabe: Am 14. Januar 2013 entweder bis 12 Uhr in den Kasten NA/02 (Kasten wird um 12 Uhr geleert!) oder bis 16.15 Uhr in der Übung, NA 5/99

AUFGABE 1 (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 *variabler* Länge:

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

$\mathsf{Mac}_k(m)$: Für $k \in \{0,1\}^n$ und $m = m_1, \ldots, m_\ell \in (\{0,1\}^{(n-1)/3})^\ell$ wähle $r \in_R \{0,1\}^{(n-1)/3}$,

$$t_i \leftarrow \mathsf{Mac}'_k(r, i, m_i, 0) \text{ für } i = 1, \ldots, \ell - 1 \text{ und}$$

$$t_\ell \leftarrow \mathsf{Mac}'_k(r, i, m_i, 1),$$

wobei i in $\{0,1\}^{(n-1)/3}$-Strings kodiert wird. Gib $t := (r, t_1, \ldots, t_\ell)$ zurück.

Im Vergleich zur Konstruktion aus der Präsenzübung wird hier ein zusätzliches Bit einkodiert. Für alle Blöcke, bis auf den letzten, ist es 0. Im letzten Block wird es auf 1 gesetzt. Im Vergleich zur Vorlesung wird aber auch hier die Länge ℓ nicht einkodiert.

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

(b) Zeigen Sie, dass Π sicher ist.

Hinweis: Orientieren Sie sich in (b) an dem Beweis aus der Vorlesung (Folie 110 ff.).

Bitte wenden!

AUFGABE 2 (5 Punkte)**:**

Sei $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine Pseudozufallsfunktion. Betrachten Sie eine Variante $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ des CBC-MAC aus der Vorlesung (Folie 117) für *variable* Nachrichtenlänge:

$\mathsf{Gen}(1^n)$: Gib $k \in_R \{0,1\}^n$ zurück.

$\mathsf{Mac}_k(m)$: Für $k \in \{0,1\}^n$ und $m = m_1, \ldots, m_\ell \in (\{0,1\}^n)^\ell$ setze $t_0 := 0^n$,

$$t_i := F_k(t_{i-1} \oplus m_i) \text{ für } i = 1, \ldots, \ell$$

und $t_{\ell+1} := F_k(t_\ell \oplus \ell)$, wobei $\ell \in \{0,1\}^n$ kodiert wird. Gib $t := t_{\ell+1}$ zurück.

In dieser Variante wird die Länge der Nachricht folglich *hinten* angehangen.

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

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

Hinweis: Aufgabenteil (b) lässt sich mit zwei Anfragen lösen. Nutzen Sie aus, dass Nachrichten unterschiedlicher Länge ℓ angefragt werden dürfen.

AUFGABE 3 (5 Punkte)**:**

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

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 4 (5 Punkte)**:**

Sei (Gen', H) eine kollisionsresistente Hashfunktion variabler Eingabelänge, die mit Hilfe der Merkle-Damgard-Transformation konstruiert wurde. Sei $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ ein MAC für *variable* Nachrichtenlänge mit:

$\mathsf{Gen}(1^n)$: Wähle $k' \in_R \{0,1\}^n, s \leftarrow \mathsf{Gen}'(1^n)$ und gib $k := (k', s)$ zurück.

$\mathsf{Mac}_k(m)$: Gib $H_s(k', m)$ zurück.

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

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

Hinweis: Nutzen Sie aus, dass dem Angreifer der öffentliche Parameter s bekannt ist.