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

Hausübungen zur Vorlesung

Kryptographie I

WS 2012/13

Blatt 7 / 14. Januar 2013

Abgabe: Am 28. 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)**:**

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

$$k \mapsto h_s(\mathsf{IV}, k \oplus \mathsf{opad}), h_s(\mathsf{IV}, k \oplus \mathsf{ipad})$$

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 (5 Punkte)**:**

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

Hinweis: Betrachten Sie $c := (\mathsf{Enc}_{k1}(m), \mathsf{Mac}_{k2}(m))$ und zeigen Sie, dass das Verfahren nicht CPA-sicher ist.

Bitte wenden!

AUFGABE 3 (5 Punkte)**:**

Zeigen Sie, dass folgende Verschlüsselungsmodi nicht CCA-sicher sind:

(a) CBC-Modus

(b) OFB-Modus

(c) CTR-Modus

AUFGABE 4 (5 Punkte)**:**

Geben Sie ein Nachrichtenübertragungsverfahren an, das *authentisierte Kommunikation* (siehe Folie 145) bietet, aber kein *sicheres* Nachrichtenübertragungsverfahren (siehe Folie 145) ist. Zeigen Sie die erste Eigenschaft und geben Sie für die zweite Eigenschaft einen Angreifer an.

Hinweis: Erweitern Sie den Chiffretext γ eines sicheren Nachrichtenübertragungsverfahrens um ein Bit.