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 5 / 20./22. Dezember 2010

AUFGABE 1. CCA-Sicherheit.
Zeigen Sie, dass keiner der folgenden „Modes of Operation“ CCA-sicher ist. Geben Sie hierzu jeweils den CCA-Angreifer an!

a) Cipher Block Chaining (CBC) Modus

b) Output Feedback (OFB) Modus

AUFGABE 2. MAC-Kandidat.
Sei $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine Pseudozufallsfunktion. Betrachten Sie den folgenden MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ für Nachrichten fester Länge $m \in \{0,1\}^{2n-2}$.

$\mathsf{Gen}(1^n)$ gibt $k \in_R \{0,1\}^n$ aus.

$\mathsf{Mac}_k(m)$ berechnet für eine Nachricht $m = (m_0, m_1)$ mit $|m_0| = |m_1| = n-1$ den Tag

$$t = \langle F_k(0||m_0), F_k(1||m_1) \rangle \ .$$

Geben Sie die Vrfy-Funktion an. Ist Π sicher?

AUFGABE 3. Drehwurm.
Sei $* : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine beliebige kommutative Verknüpfung, d.h. $x * y = y * x$ für alle $x, y \in \{0,1\}^n$. Sei $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ eine Pseudozufallsfunktion. Betrachten Sie den folgenden MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$.

$\mathsf{Gen}(1^n)$ gibt $k \in_R \{0,1\}^n$ aus.

$\mathsf{Mac}_k(m)$ berechnet für eine Nachricht $m = (m_1, \ldots, m_\ell) \in (\{0,1\}^n)^\ell$ den Tag

$$t = F_k(m_1) * \ldots * F_k(m_\ell) \ .$$

$\mathsf{Vrfy}_k(m,t)$ gibt 1 aus genau dann, wenn $t = F_k(m_1) * \ldots * F_k(m_\ell)$.

Zeigen Sie, dass Π unsicher ist.