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

Hausübungen zur Vorlesung

Kryptographie I

WS 2012/13

Blatt 5 / 30. November 2012

Abgabe: Am 17. Dezember 2012 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)**:**

Zeigen Sie, dass die Konstruktion Π_B (Folie 73) auch CPA-sicher ist, falls (statt einer Pseudozufallsfunktion) eine *schwache Pseudozufallsfunktion* (siehe Präsenzübung) verwendet wird.

AUFGABE 2 (5 Punkte)**:**

Betrachten Sie eine Variante des CBC Modus, in der $\mathsf{IV}_0 \in_R \{0,1\}^n$ gewählt wird, aber dann für jede neue Verschlüsselung i der zugehörige IV_i mit Hilfe einer *bekannten* Funktion $h : \{0,1\}^n \to \{0,1\}^n$ als $\mathsf{IV}_i := h(\mathsf{IV}_{i-1})$ aus dem vorherigen IV_{i-1} bestimmt wird.

Zeigen Sie, dass dieser modifizierte CBC-Modus nicht CPA-sicher ist.

AUFGABE 3 (5 Punkte)**:**

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 $m \in \{0,1\}^{2n-2}$ fester Länge.

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

$\mathsf{Mac}_k(m)$: Berechnet für $m = (m_0, m_1)$ mit $|m_0| = |m_1| = n-1$, $r \in_R \{0,1\}^n$ den Tag

$$t := (r, F_k(r) \oplus F_k(m_0, 0) \oplus F_k(m_1, 1)).$$

Geben Sie eine korrekte Vrfy-Funktion an. Zeigen Sie, dass Π nicht sicher ist.

AUFGABE 4 (5 Punkte)**:**

Seien $\Pi' = (\mathsf{Gen}', \mathsf{Mac}', \mathsf{Vrfy}')$, $\Pi'' = (\mathsf{Gen}'', \mathsf{Mac}'', \mathsf{Vrfy}'')$ zwei MACs, von denen wir wissen, dass mindestens einer sicher ist. Wir wissen allerdings nicht, welcher MAC sicher ist. Konstruieren Sie aus diesen MACs einen sicheren MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$. Zeigen Sie die Korrektheit und die Sicherheit Ihrer Konstruktion.