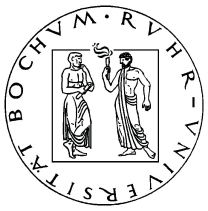
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Thomas Dullien



Hausübungen zur Vorlesung

Kryptographie I

WS 2009

Blatt 5 / 14. Dezember 2009 / Abgabe 21. Dezember 2009, 12 Uhr

AUFGABE 1 (5 Punkte)**:**
Zeigen Sie, dass der einfache CBC-MAC *nicht* sicher ist, wenn er wie auf Folie 96 erwähnt, mit variablem l konstruiert wird.

AUFGABE 2 (5 Punkte)**:**
Betrachten Sie einen sicheren MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ und für $k \in \{0,1\}^n$ den Algorithmus $\mathsf{Mac}_k : \{0,1\}^* \to \{0,1\}^{t(n)}$. Zeigen Sie: t muss super-logarithmisch sein, d.h. wenn $t(n) = \mathcal{O}(\log n)$ kann Π kein sicherer MAC sein.

AUFGABE 3 (5 Punkte)**:**
Betrachten Sie die Merkle-Damgard-Konstruktion aus der Vorlesung, und nehmen Sie an, dass der Block x_{B+1} *nicht* mit in die Berechnung einbezogen wird. Geben Sie zwei Nachrichten $x \neq x'$ an, für die $H(x) = H(x')$ gilt, und erklären Sie, welcher Schritt im Sicherheitsbeweis auf Folie 104 nicht mehr richtig funktioniert.

AUFGABE 4 (5 Punkte)**:**
Sei F eine Pseudozufallsfunktion. Zeigen Sie, dass der folgende MAC für Nachrichten der Länge $2n$ unsicher ist: Der Key sei zufällig der Länge n. Eine Nachricht der Länge $2n$ der Form $m_1||m_2$ und $|m_1| = |m_2|$ wird mittels $\langle F_k(m_1), F_k(F_k(m_2))\rangle$ authentifiziert.