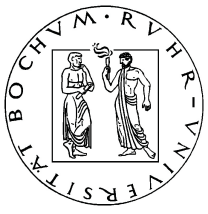
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Thomas Dullien



Präsenzübungen zur Vorlesung

Kryptographie I

WS 2009

Blatt 5 / 14. Dezember 2009

AUFGABE 1 (5 Punkte)**:**
Zeigen Sie, dass der einfache CBC-MAC *nicht* sicher ist, wenn er wie auf Folie 97 konstruiert wird (d.h. mit zufälligem t_0 und der Ausgabe von (t_0, t_l)).
Zeigen Sie, dass der einfache CBC-MAC *nicht* sicher ist, wenn die Werte $t_0, \ldots, t_{l-1}$ auch ausgegeben werden.

AUFGABE 2 (5 Punkte)**:**
Erweitern Sie dass Merkle-Damgard-Schema auf eine beliebige Kompressionsfunktion, die die Eingaben um mindestens ein Bit komprimiert. Benutzen Sie eine allgemeine Eingabelänge l' und eine allgemeine Ausgabelänge l.

AUFGABE 3 (5 Punkte)**:**
Sei (Gen, H) eine kollisionsresistente Hashfunktion. Ist $\tilde{H}^s(x) := H^s(H^s(x))$ zwangsläufig auch Kollisionsresistent ?

AUFGABE 4 (5 Punkte)**:**
Sei $\cdot : \{0,1\}^l \times \{0,1\}^l \rightarrow \{0,1\}^l$ eine beliebige kommutative Verknüpfung. Sei F eine Pseudozufallsfunktion. Zeigen Sie, dass für die Nachricht $m = m_1 || \ldots || m_l$ der MAC mit $t := \langle F(m_1) \cdot \cdots \cdot F(m_l) \rangle$ kein sicherer MAC ist.