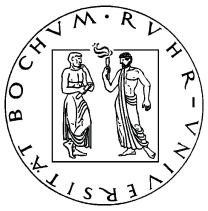
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Thomas Dullien



Hausübungen zur Vorlesung

Kryptographie I

WS 2009

Blatt 6 / 9. Januar 2010 / Abgabe 18. Januar 2010, 12 Uhr

AUFGABE 1 (5 Punkte)**:**
Geben Sie ein von dem Beispiel in der Vorlesung verschiedenes authenticate-then-encrypt-Schema an, welches unsicher ist.

AUFGABE 2 (5 Punkte)**:**
Konstruieren Sie Verschlüsselungsschema welches CCA-sicher aber kein sicheres Nachrichtenübermittlungsschema ist.

AUFGABE 3 (5 Punkte)**:**
Vor der Erfindung von HMAC war es häufig so, dass eine MAC "improvisiert" wurde, in dem $\mathsf{Mac}_k(m) = H^s(k||m)$ gesetzt wurde. Hierbei war H eine kollisionsresistente Hashfunktion. Zeigen Sie, dass dies keine sichere MAC ist wenn H per Merkle-Damgard verfahren konstruiert wurde.

AUFGABE 4 (5 Punkte)**:**
Betrachten Sie ein Schema, welches aus einer sicheren Mac mit eindeutigen Tags sowie sowie einer CPA-sicheren Verschlüsselung Enc besteht. Es wird das Paar $\langle \mathsf{Enc}_{k_1}(m), \mathsf{Mac}_{k_2}(m) \rangle$ übertragen. Zeigen Sie, dass das resultierende Schema nicht CPA-sicher ist.