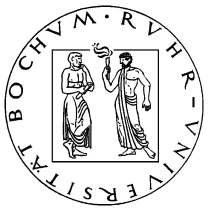
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann



Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2009

Blatt 6 / 8. Juli 2009

AUFGABE 1:
Wir betrachten das Lamport One-Time Signaturschema. Beschreiben Sie einen Angreifer, der Signaturen von zwei Nachrichten seiner Wahl erhält und anschließend Signaturen für beliebige Nachrichten fälschen kann.

AUFGABE 2:
Zeigen Sie, dass die Existenz eines One-Time Signaturschemas für 1-bit Nachrichten die Existenz von Einwegfunktionen impliziert.

AUFGABE 3:
Ein **starkes** One-Time Signaturschema erfüllt die folgende Eigenschaft: Es ist nicht möglich, gegeben eine Signatur σ einer Nachricht m, ein Paar $(m', \sigma') \neq (m, \sigma)$ auszugeben, so dass σ' eine gültige Signatur für m' ist (insbesondere ist $m' = m$ erlaubt).

1. Angenommen es existieren Einwegfunktionen. Geben Sie eine Einwegfunktion an, für die Lamports Signaturschema **nicht** die Eigenschaft eines starken One-Time Signaturschemas erfüllt.

2. Geben Sie eine Idee für die Konstruktion eines starken One-Time Signaturschemas an. Benutzen Sie dabei eine bestimmte Einwegfunktion im Lamport-Verfahren.