Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Dr. Christopher Wolf
Alexander Meurer, Florian Giesen

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2010

Blatt 4 / 8. Juni 2010

AUFGABE 1. Hash-Varianten.
Anstelle von Kollisionsresistenz reicht es in manchen Anwendungen aus, schwächere Forderungen an eine Hashfunktion zu stellen. Man nennt eine Hashfunktion $\Pi_H = (\mathsf{Gen}, H)$ *urbildresistent*, wenn es zu gegebenem $s \leftarrow \mathsf{Gen}(1^n)$ und $y \leftarrow H^s(x)$ für $x \in_R \{0,1\}^*$ unmöglich ist, ein $x' \in \{0,1\}^*$ mit $H^s(x') = y$ zu berechnen.

a) Formalisieren Sie die Definition der *Urbildresistenz* durch Angabe eines geeigneten Spiels und definieren Sie den Vorteil eines Urbild-Angreifers.

b) Zeigen Sie, dass *Kollisionsresistenz* die *Urbildersistenz* impliziert.

AUFGABE 2. Doppelter Lamport.
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 3. Alternativer Lamport.
Das Lamport One-Time Signaturverfahren benutzt 2ℓ Werte im öffentlichen Schlüssel um Nachrichten der Länge ℓ zu signieren. Betrachten Sie die folgende Variante:

- Der private Schlüssel besteht aus 2ℓ Werten $x_1, \ldots, x_{2\ell}$
- Der öffentliche Schlüssel beinhaltet die Werte $y_1, \ldots, y_{2\ell}$ mit $y_i = f(x_i)$
- Eine Nachricht $m \in \{0,1\}^{\ell'}$ wird 1-zu-1 auf eine Teilmenge $S_m \subset \{1, \ldots, 2\ell\}$ der Größe ℓ abgebildet. Um eine Nachricht zu signieren veröffentlicht der Signierer $\{x_i\}_{i \in S_m}$.

Hierbei ist f eine Einwegfunktion. Zeigen Sie, dass dieses Verfahren ein One-Time Signaturverfahren ist indem Sie das Invertieren von f auf das Fälschen einer Signatur reduzieren. Was ist die maximale Nachrichtenlänge ℓ' für dieses System?