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

RUHR UNIVERSITÄT BOCHUM RUB

Hausübungen zur Vorlesung

Kryptographie 2

SS 2010

Blatt 4 / 8. Juni 2010 / Abgabe 16. Juni, 12:30 Uhr, Kasten NA 02

AUFGABE 1. Mindmap. (10 Punkte)
Erstellen Sie ein Schaubild zum ersten Themenblock der Vorlesung über *Schlüsselaustausch* und *Public Key Verschlüsselung*. Wiederholen Sie hierzu

- wesentlichen Definitionen (z.B. *CPA-Sicherheit* oder zugrundeliegende *Sicherheitsannahmen*)
- konkrete Verschlüsselungsverfahren (z.B. ElGamal)
- Konstruktionen (z.B. *hybride Verschlüsselung*)

und stellen Sie eine geeignete Auswahl kompakt dar. Versuchen Sie auch, bestehende Zusammenhänge zu skizzieren (z.B. Konstruktion von *1-Bit Verschlüsselung* mittels *Hardcore-Prädikat* und generische Transformation auf *Multi-Bit Verschlüsselung*).

AUFGABE 2. Hashfunktionen. (5 Punkte)
Seien (Gen_1, H_1) und (Gen_2, H_2) zwei Hashfunktionen. Wir konstruieren daraus eine weitere Hashfunktion (Gen, H) wie folgt:

- $\mathsf{Gen}(1^n)$ gibt (s_1, s_2) aus mit $s_1 \leftarrow \mathsf{Gen}_1(1^n)$ und $s_2 \leftarrow \mathsf{Gen}_2(1^n)$
- $H^{(s_1,s_2)}(x) := H_1^{s_1}(x)||H_2^{s_2}(x)$.

a) Zeigen Sie, dass wenn mindestens eine der beiden Hashfunktionen (Gen_1, H_1) oder (Gen_2, H_2) *kollisionsresistent* ist, so ist auch (Gen, H) *kollisionsresistent*.

b) Beweisen oder widerlegen Sie eine analoge Aussage für den Fall der *Urbildresistenz* (siehe Präsenzübung), d.h. überlegen Sie ob (Gen, H) *urbildresistent* ist, falls mindestens eine der beiden Hashfunktionen (Gen_1, H_1) oder (Gen_2, H_2) urbildresistent ist.

AUFGABE 3. Einmalsignaturen. (5 Punkte)
Sei f eine Einwegpermutation. Wir betrachten das folgende Signaturschema für Nachrichten aus der Menge $\{1, \ldots, n\}$:

- Für die Schlüsselerzeugung wird ein zufälliges $x \in \{0,1\}^n$ gewählt und $y := f^n(x)$ berechnet.[1] Der öffentliche Schlüssel ist nun y und der private Schlüssel ist x.
- Um eine Nachricht $i \in \{1, \ldots, n\}$ zu signieren wird die Signatur $f^{n-i}(x)$ ausgegeben (wobei $f^0(x) = x$).
- Eine Signatur σ für eine Nachricht i bezüglich des öffentlichen Schlüssels y wird verifiziert indem geprüft wird, ob $y \stackrel{?}{=} f^i(\sigma)$.

a) Zeigen Sie, dass das vorgestellte Verfahren kein One-Time Signaturschema ist.

Gegeben sei eine Signatur für Nachricht i, für welche Nachrichten j kann ein Angreifer eine Fälschung erzeugen?

b) Zeigen Sie, dass es keinen ppt. Angreifer gibt, der aus einer Signatur für Nachricht i eine Fälschung für irgendeine Nachricht $j > i$ berechnet (ausser mit vernachlässigbarer Wahrscheinlichkeit).

c) Wie kann das angegebene Verfahren modifiziert werden um ein One-Time Signaturverfahren zu erhalten?

Hinweis: Benutzen Sie zwei Werte y, y' im öffentlichen Schlüssel.

[1] Hierbei ist $f^n(x) = f(f(\ldots f(x))\ldots)$ die n-fache Komposition von f