Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Eike Kiltz
Gottfried Herold

Hausübungen zur Vorlesung

Kryptographie I

WS 2011/2012

Blatt 6 / 10. Januar 2012 / Abgabe **bis spätestens Montag, 23.01.2012 16:00 Uhr**

AUFGABE 1:

Betrachten Sie die folgende Hashfunktion $(\mathbf{Gen}, H)$ mit $H : \{0,1\}^{n+1} \to \{0,1\}^n$, die um 1 Bit komprimiert.

- $\mathbf{Gen}(1^n)$ wählt eine zufällige $n \times (n+1)$-Matrix $S \in \mathbb{F}_2^{n,n+1}$ mit Rang n.
- $H_S(x)$ für $x \in \{0,1\}^{n+1}$ ist definiert durch $H_S(x) = S \cdot x$, wobei $S \cdot x$ das Matrix-Vektor Produkt bezeichnet und $x \in \{0,1\}^{n+1}$ als $\mathbb{F}_2^{n+1}$ interpretiert wird.

Zeigen Sie, dass diese Hashfunktion nicht kollisionsresistent ist. [3 Punkte]

AUFGABE 2:

Sei $(\mathbf{Gen}, h)$ eine kollisionsresistente Hash-Funktion mit $h : \{0,1\}^{2\ell} \to \{0,1\}^{\ell}$.
Betrachten Sie die folgende Variation $\hat{H}_s : \{0,1\}^* \to \{0,1\}^{2\ell}$ der Merkle-Damgård-Konstruktion (Notation wie im Skript):
Anstatt im letzten Schritt $z_{B+1} = h_s(z_B \mid\mid x_{B+1})$ auszugeben, wird direkt $z_B \mid\mid x_{B+1}$ ausgegeben.

Zeigen Sie direkt, dass dies weiterhin eine kollisionsresistente Hashfunktion liefert. [5 Punkte]

Bemerkung:
Der Sinn der Aufgabe ist, dass Sie den Beweis der Kollisionsresistenz der Merkle-Damgård-Konstruktion nochmal nachvollziehen. Daher sollen Sie die Kollisionsresistenz direkt zeigen, und nicht auf die Kollisionsresistenz der Merkle-Damgård-Konstruktion reduzieren.

- bitte wenden -

AUFGABE 3:

Sei $(\mathbf{Gen}, H)$ eine Hashfunktion, die mittels der Merkle-Damgård-Konstruktion aus der kollisionsresistenten Hashfunktion $(\mathbf{Gen}, h)$ hervorging. Zeigen Sie, dass der folgende MAC $\Pi = (\mathbf{Gen}', \mathbf{Mac}, \mathbf{Vrfy})$ *nicht* sicher ist [5 Punkte]:

- $\mathbf{Gen}'(1^n)$: $s \leftarrow \mathbf{Gen}(1^n)$ und $k \in_R \{0,1\}^n$ uniform. Der Schlüssel ist $k' = (s, k)$.
- $\mathbf{Mac}_{(s,k)}(m)$: Gibt $t = H_s(k \,||\, m)$ aus.
- $\mathbf{Vrfy}_{(s,k)}(t, m)$: Prüft, ob $t = H_s(k \,||\, m)$ ist.

Wir nehmen hierbei an, dass s öffentlich ist, d.h. dem Angreifer bekannt.

Bemerkung:
Konstruktionen diesen Typs wurden vor der Entwicklung von HMAC in der Praxis angewandt.

AUFGABE 4:

(a) Sei $(\mathbf{Gen}, h)$ kollisionsresistene Hash-Funktion mit $h_s : A \to B$
(z.B. $A = \{0,1\}^*, B = \{0,1\}^\ell$). Weiterhin seien $x_0 \in A, y_0 \in B$ zwei öffentliche Konstanten.
Wir definieren eine neue Hashfunktion $(\mathbf{Gen}, h')$ mit dem selben **Gen** durch:

$$h'_s(x) := \begin{cases} y_0 & \text{falls } h_s(x) = h_s(x_0) \\ h_s(x_0) & \text{falls } h_s(x) = y_0 \\ h_s(x) & \text{sonst.} \end{cases}$$

Zeigen Sie, dass $(\mathbf{Gen}, h')$ kollisionsresistent ist. [2 Punkte]
Bemerkung: Durch diese Konstruktion wird erreicht, dass $h'_s(x_0) = y_0$ für alle s gilt.

(b) Betrachten Sie die folgende Variante der Merkle-Damgård-Konstruktion. Sei $(\mathbf{Gen}, h)$ kollisionsresistente Hashfunktion mit $h_s : \{0,1\}^{2\ell} \to \{0,1\}^\ell$.

Wir konstruieren $(\mathbf{Gen}, H)$ (mit dem selben **Gen**) wie folgt:
$H_s(x)$ für $x \in \{0,1\}^L$ ist definiert durch:

1. Schreibe $x = x_1 \,||\, \ldots \,||\, x_B$ mit $x_i \in \{0,1\}^\ell$, wobei x ggf. durch 0en ergänzt wird.
2. Setze $z_0 := IV = L$ und $z_i := h_s(z_{i-1} \,||\, x_i)$ für $i \leq B$.
3. Gib z_B aus.

Zeigen Sie, dass H *nicht notwendigerweise* kollisionsresistent ist. [5 Punkte]

Hinweis: Mittels des Tricks aus (a) können Sie o.B.d.A. annehmen, dass $h_s(x_0) = y_0$ gilt für von Ihnen geeignet gewähltes x_0, y_0. Geben Sie für so ein h dann einen Angriff auf die Kollisionsresistenz von H an.