TECHNISCHE UNIVERSITÄT BERLIN Sommersemester 2004
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. Heß
WM: Dipl.-Math. M. Wagner
`www.math.tu-berlin.de/~hess/krypto`

4. Übung Kryptographie

1. Aufgabe Floyds Algorithmus (4 Punkte)

Sei $p \in \mathbb{N}$ und $f : \{0, \ldots, p-1\} \longrightarrow \{0, \ldots, p-1\}$ eine beliebige Funktion. Wir definieren eine Folge $x_0, x_1, \ldots$ wie folgt: Wähle $x_0 \in \{0, \ldots, p-1\}$ zufällig und $x_{i+1} = f(x_i)$ für $i \geq 0$.

(a) Begründen Sie, warum es $l, t \in \mathbb{N}$ mit $l + t \leq p + 1$ gibt, so daß $x_i = x_{i+l}$ für alle $i \geq t$ gilt.

(b) Sei $(y_i)_{i \in \mathbb{N}}$ eine weitere Folge, für die gilt: $y_0 = x_0$ und $y_{i+1} = f(f(y_i))$ für $i \geq 0$. Zeigen Sie: Es gibt $i_0 \leq t + l$, so daß gilt: $x_{i_0} = y_{i_0}$.

2. Aufgabe Hashfunktionen, Merkles Meta Methode (4 Punkte)

(a) Sei g eine kollisionsresistente Hashfunktion mit $g : \{0,1\}^* \longrightarrow \{0,1\}^n$ und h wie folgt definiert:

$$h : \{0,1\}^* \longrightarrow \{0,1\}^{n+1}, \quad h(x) = \begin{cases} 1\|x & \text{wenn x Bitlänge } n \text{ hat} \\ 0\|g(x) & \text{sonst.} \end{cases}$$

Zeigen Sie, daß h keine Einwegfunktion ist.

(b) Welche Auswirkungen hat es, wenn man in Merkles Meta Methode (oder in der Merkle-Damgard Konstruktion) die Bitlänge nicht kodiert, also nur ein geeignetes Padding macht? Welche Grössenbedingung sollte man an den Bildbereich einer Hashfunktion stellen?

3. Aufgabe Stromchiffre, LFSR (4 Punkte)

Ein LFSR der Länge n und der Anfangsbelegung $a = (a_0, \ldots, a_n) \in \{0,1\}^n$ sei gegeben durch

$$z_{i+n} = \bigoplus_{j=0}^{n-1} a_j \cdot z_{i+j} \quad (i \geq 0).$$

Welche der folgenden Bitsequenzen $(x_0, \ldots, x_9)$ können von einem LFSR der Länge 5 erzeugt worden sein? Geben Sie gegebenenfalls die Anfangsbelegung an.

(a) 0000010001

(b) 0000100001

(c) 0000100011

(d) 0001000001

4. Aufgabe Geburtstagsattacke **(8 Punkte)**

Alice möchte an Bob eine Mail schicken, in der festgehalten wird, daß Bob das Auto von Alice für 1000 Euro kauft. Die Mail enthält einen Header. Alice hat herausbekommen, daß dieser Header noch aus alten Zeiten stammt. Mail-Programme die heutzutage in Gebrauch sind benutzen diesen Header nicht mehr. Wohl aus Bequemlichkeit hat man diese nicht entfernt. In einer zweiten fingierten Mail schreibt Alice, daß der Verkaufspreis 10000 Euro beträgt statt 1000. Nun versucht Alice, die fingierte Nachricht im Header so abzuändern, daß sie den gleichen Hashwert hat wie die ursprüngliche Nachricht. In der Datei AliceMail auf der Kryptographie-Homepage ist eine Hashfunktion SHA1 vorgegeben, welche beliebige Strings auf Hexadezimalstrings der Länge 6 abbildet. Es gibt zwei Mails, eine Original-Mail und eine Fälschung. Finden Sie mit Hilfe der Geburtstagsattacke eine Kollision, so daß die fingierte Mail den gleichen Hashwert hat wie die Ursprüngliche.

Achtung: Die Hashfunktion SHA1 funktioniert nur unter Linux/Unix

Gesamt: 20 Punkte