TECHNISCHE UNIVERSITÄT BERLIN WS06/07
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr.F. Heß
WM: Dipl.-Math. M. Wagner
`www.math.tu-berlin.de/~hess/krypto-ws2006`

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 und Merkle-Damgard (6 Punkte)

(a) Was kann über das Verhältnis der folgenden beiden Eigenschaften einer Hashfunktion

$$H : \{0,1\}^* \longrightarrow \{0,1\}^n$$

gesagt werden:

(i) H ist eine Einwegfunktion

(ii) H ist kollisionsresistent

(b) Wie sieht es mit der Sicherheit von folgenden modifizierten Merkle-Damgard Hashfunktionen bezüglich der Kompressionsfunktion aus:

(i) Es wird kein padding verwendet.

(ii) Es werden iterierte Paddings wie im Skript beschrieben verwendet und dürfen beliebige Länge haben (d.h. für kurze Eingaben kurz, für lange lang).

(iii) Es werden iterierte Paddings wie im Skript beschrieben verwendet, aber die Anzahl der Iterierungen (also die Länge) ist für alle Nachrichten gleich.

3. Aufgabe LFSR **(4 Punkte)**

Sei $C(t) = 1 + \sum_{i=1}^{n} c_i t^i \in \mathbb{F}_2[t]$ und $n \in \mathbb{N}$ gegeben. Über die Funktion

$$f : \{0,1\}^n \longrightarrow \{0,1\}, \quad s = (s_{n-1}, \ldots, s_1, s_0) \longmapsto c_1 s_{n-1} + \ldots + c_{n-1} s_1 + c_n s_0$$

sind die Zustände $(s_n, s_{n-1} \ldots, s_1)$ mit $s_n := f(s)$ gegeben. Wir können f mit einer geeigneten Matrix $A \in \mathbb{F}_2^{n \times n}$ beschreiben so dass die Zustände durch $s, sA, sA^2, sA^3, \ldots$ gegeben sind. Zeige folgende Aussagen:

(a) Für das charakteristische Polynom $p(t) \in \mathbb{F}_2[t]$ von A gilt $p(t) = t^n C(\frac{1}{t})$

(b) Ist $C(t)$ irreduzibel so auch $p(t)$

(c) Die Menge der von $s = 0$ verschiedenen Zustände wird durch den LFSR, der durch $(C(t), n)$ definiert ist, in disjunkte Perioden zerlegt.

(d) Ist $s = s_0, s_1, s_2 \ldots,$ eine periodische binäre Folge mit Periodenlänge n, so ist s die Ausgabefolge des LFSR der von $(n, 1 + t^n)$ mit Anfangszustand $(s_{n-1}, \ldots, s_1, s_0)$ erzeugt wird.

4. Aufgabe LFSR: Komplexität **(6 Punkte)**

Zeige folgende Aussagen:

(a) Finde $n \in \mathbb{N}$ und $C(t) \in \mathbb{F}_2[t]$ geeignet so, dass davon der Strom $s = 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1 \ldots$ erzeugt wird. Wie gross ist die Komplexität $L(s)$?

(b) Finde $n \in \mathbb{N}$ und $C(t) \in \mathbb{F}_2[t]$ geeignet so, dass davon der Strom $s = 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1 \ldots$ erzeugt wird. Wie gross ist die Komplexität $L(s)$?

Zeige, dass wenn $s = s_1, s_2, \ldots$ eine periodische binäre Folge mit Periodenlänge $m \in \mathbb{N}$ ist dann für die Komplexität folgende Abschätzung gilt:

$$L(s) \leq m \leq 2^{L(s)-1}.$$

Gesamt: 20 Punkte