TECHNISCHE UNIVERSITÄT BERLIN WS 2007-2008
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. Florian Heß
Assistent: Osmanbey Uzunkol
www.math.tu-berlin.de/∼hess/krypto-ws2007

Abgabe: 09.11.2007
in der Übung

3. Übung Kryptographie

(Stromchiffren, LFSR, Hashfunktionen, Floyd's Algorithmus)

---

1. Aufgabe

Gegeben seien folgende Schlüsselstrome:

$$\alpha = 00100001111101010011000100001111101010011000100001,$$
$$\beta = 00110000110110111001101001011010111101111011101111,$$
$$\gamma = 10011111000100001101010110011111000100001101010110 0.$$

Unter diesen 3 Schlüsselfolgen wurden eine mittels LFSR erzuegt, die andere mittels linearer Kongruenzgeneratoren erzeugt und die eine zufällig gegeben.

(a) Die mittels LFSR konstruierte Folge hat die minimale Länge l. Bestimmen Sie welche der oben gegebenen Folgen mittels LFSR konstruiert ist. Ferner finden Sie die geeigneten $a_1, \ldots, a_l$ mit kleinstem l, wobei die wie im Skript definiert sind.

(b) Die mittels linearer Kongruenzgeneratoren konstruierte Folge wurde im Ring $\mathbb{Z}/8\mathbb{Z}$ erzeugt, und entsprechende Werte werden in binärer Darstellung geschrieben, das heißt $0 \to 000, 1 \to 001, \cdots, 7 \to 111$. Bestimmen welche der oben gegebenen Folgen mittels linearer Kongruenzgeneratoren konstruiert ist. Ferner Finden Sie die in der Vorlesung eingeführten Parameter a und b.

(8 Punkte)

2. Aufgabe

Was kann über das Verhältnis der folgenden beiden Eigenschaften einer Hashfunktion

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

gesagt werden:

(a) H ist eine Einwegfunktion,

(b) H ist kollisionsresistent.

(3 Punkte)

3. Aufgabe

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, dass es $i_0 \leq t + l$ gibt, so dass $x_{i_0} = y_{i_0}$ gilt.

(4 Punkte)