TECHNISCHE UNIVERSITÄT BERLIN WS08/09
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. Heß
Assistent: G. Möhlmann
Abgabe: 11.11.08
www.math.tu-berlin.de/~hess/krypto-ws2008

3. Übung Kryptographie

1. Aufgabe

Gegeben seien folgende Schlüsselströme:

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

Unter diesen 3 Schlüsselfolgen wurde eine mittels LFSR, eine andere mittels linearer Kongruenzgeneratoren und die verbleibende zufällig erzeugt.

(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 Notation wie im Skript ist.

(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.

(5 Punkte)

2. 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) Gilt die Aussage auch für $l + t \leq p$?

(c) 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 $1 \leq i_0 \leq t + l$ gibt, so dass $x_{i_0} = y_{i_0}$ gilt.

(5 Punkte)

3. Aufgabe

Betrachten Sie die Folgen, die ein linearer Kongruenzgenerator durch $x_{i+1} = ax_i + b \mod m$ fuer einen Startwert $0 \leq x_0 \leq m-1$ erzeugt.Bezeichne r_{x_0} die Periodenlänge der Folge zum Startwert x_0. Beweisen oder widerlegen Sie:

(a) Gilt $r_{x_0} = m$ für einen speziellen Startwert x_0, so auch für alle anderen Startwerte.

(b) Sind b und m nicht teilerfremd, so gilt $r_{x_0} < m$ für alle Startwerte x_0.

(c) Sind b und m teilerfremd, so gilt $r_{x_0} = m$ für alle Startwerte x_0.

(5 Punkte)

4. Aufgabe

Implementieren Sie AES. Dazu können Sie die vorgegebenen Funktionen aus AES.k verwenden.

(5 Punkte)