TECHNISCHE UNIVERSITÄT BERLIN WS08/09
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. Heß
Assistent: G. Möhlmann
Abgabe: 18.11.08
www.math.tu-berlin.de/~hess/krypto-ws2008

4. Übung Kryptographie

1. Aufgabe

Sei h eine Kompressionsfunktion, welche einen n-Bitstring auf einen m-Bitstring abbildet. Wir können daher die Funktion h als eine Funktion von $\mathbb{Z}/2^n\mathbb{Z}$ nach $\mathbb{Z}/2^m\mathbb{Z}$ interpretieren.

(a) Ferner seien $n = m$ und $h : \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/2^n\mathbb{Z}$ wie folgt definiert:

$$h(x) := x^2 + ax + b \bmod 2^n.$$

Zeigen Sie, dass es einfach ist eine Kollision zu gegebenem $x_0 \in \mathbb{Z}/2^n\mathbb{Z}$ zu finden ohne die quadratische Gleichung in $\mathbb{Z}/2^n\mathbb{Z}$ lösen zu müssen.

(b) Es seien nun $n > m$ und $h : \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{Z}/2^m\mathbb{Z}$ wie folgt definiert:

$$h(x) := \sum_{i=0}^{d} a_i x^i \bmod 2^m,$$

wobei $a_i \in \mathbb{Z}$ für $0 \leq i \leq d$ sind. Zeigen Sie, dass es einfach ist eine Kollision zu gegebenem $x_0 \in \mathbb{Z}/2^n\mathbb{Z}$ zu finden ohne die Polynomgleichung in $\mathbb{Z}/2^m\mathbb{Z}$ lösen zu müssen.

(5 Punkte)

2. Aufgabe

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 $p(t)$

(3 Punkte)

3. Aufgabe

Zeige folgende Aussagen:

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

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

Sei $s = s_1, s_2, \ldots$ eine periodische binäre Folge mit Periodenlänge $m \in \mathbb{N}$. Geben Sei ein Polynom $C(t) \in \mathbb{F}_2[t]$ vom Grad m an, das diese Folge erzeugt.

(6 Punkte)

4. Aufgabe

Alice schickt an Bob eine Mail, in der festgehalten wird, daß Bob das Auto von Alice für 1000 Euro kaufen möchte. 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 diesen 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.k ist eine Hashfunktion SHA1Light vorgegeben, welche beliebige Strings auf Hexadezimalstrings der Länge 7 abbildet. Es gibt zwei Mails, eine Original-Mail und eine Fälschung. Finde mit Hilfe der Geburtstagsattacke eine Kollision, so daß die fingierte Mail den gleichen Hashwert hat wie die ursprüngliche Mail.

(6 Punkte)