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: 16.11.2007
in der Übung

4. Übung Kryptographie

(Polynomielle Algorithmen, Geburtstagsangriff, Hashfunktionen, SHA1, MAC)

---

1. Aufgabe

Eine Funktion $f : \mathbb{R}^{\geq 0} \to \mathbb{R}$ heißt polynomiell (in k), wenn es ein Polynom $P \in \mathbb{R}^{\geq 0}[x]$ und $k_0 \in \mathbb{R}^{\geq 0}$ gibt, so dass $|f(k)| \leq P(k)$ für alle $k \geq k_0$.
Eine Funktion $f : \mathbb{R}^{\geq 0} \to \mathbb{R}$ heißt vernachlässigbar (in k), wenn es für jedes Polynom $Q \in \mathbb{R}^{\geq 0}[x]$ ein $k_0 \in \mathbb{R}^{\geq 0}$ gibt, so daß $|f(k)| \leq 1/Q(k)$ für alle $k \geq k_0$.

- Geben Sie eine vernachlässigbare Funktion an, deren sämtliche Funktionswerte ungleich Null sind.

Ein Algorithmus heißt polynomiell, wenn seine Laufzeit in Abhängigkeit der Bitlänge seiner Eingabe eine polynomielle Funktion ist.
Sei M eine Menge von 2^n Bitstrings der Länge n. Wir betrachten den folgenden Algorithmus A: Unter Eingabe von $m_0 \in M$ und $s \in \mathbb{Z}^{\geq 0}$ wählt A maximal s zufällig und gleichverteilte $m \in M$. Gilt $m = m_0$, wird abgebrochen und das Ergbnis 1 zurückgeliefert, ansonsten das Ergebnis 0.

- Bestimmen Sie $\Pr(A(m_0, s) = 1 : m_0 \leftarrow M)$, wobei $m_0 \leftarrow M$ bedeutet, dass m_0 zufällig und gleichverteilt aus M gewählt wird.
- Zeigen Sie, dass es kein $s \in \mathbb{Z}^{\geq 0}$ gibt, so dass A polynomiell ist und das Ergebnis 1 mit nicht vernachlässigbarer Wahrscheinlichkeit zurückliefert.

(5 Punkte)

2. Aufgabe

(a) Argumentieren Sie, wie es mit der Sicherheit von folgenden modifizierten Merkle-Damgard Hashfunktionen bezüglich der Kompressionsfunktion aussieht:

- Es wird kein padding verwendet.
- Es werden Paddings wie im Skript beschrieben verwendet und dürfen beliebige Länge haben (d.h. für kurze Eingaben kurz, für lange lang).
- Es werden Paddings wie im Skript beschrieben verwendet, aber die Anzahl der Iterierungen (also die Länge) ist für alle Nachrichten gleich.

(b) Argumentieren Sie, wie die Ausgabeblocklängen m von g und n von h im Verhältnis zueinander dimensioniert werden sollten, um ein optimales Effizienz/Sicherheitsverhältnis gemäss der Reduktion des Satzes über geschachtelte MACs im Idealfall zu erhalten? Begründen Sie Ihre Antwort!

(5 Punkte)

3. Aufgabe

Sei h eine Kompressionsfunktion, welche ein 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.

- 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.

- 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)

4. Aufgabe

Alice schickt an Bob als ein Kaufvertrag eine Email mit dem digitalen Unterschrifft σ, in der festgehalten wird, dass Bob das Auto von Alice für 1000 Euro kaufen möchte. Der digitale Unterschrifft σ von Alice hängt von einem geheimen Schlüsel von ihr und dem Hashwert der verwendeten Hashfunktion ab. Die Mail enthält einen Header, welcher einen Eintrag mit einer zufälligen Seriennummer ist. 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 Euro. 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 auf der Kryptographie-Homepage ist eine Hashfunktion SHA1Light 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 Mail.

Hinweis: Sie können diese Aufgabe bis 16.11.2007 abgeben.

(8 Punkte)