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

3. Übung Kryptographie

1. Aufgabe **Endliche Körper** **(4 Punkte)**

(i) Sei $p = 29947$ und $b = 10029$ gegeben. Berechnen Sie $b^{-1} \in \mathbb{Z}/p\mathbb{Z}$ mit Hilfe des erweiterten euklidischen Algorithmus. Schreiben Sie jeden Rechenschritt auf.

(ii) Im Rijndael-Verfahren (AES) wird in einem endlichen Körper $K := \mathbb{F}_{2^8}$ gerechnet. Dazu wird ein festes Polynom $f = x^8 + x^4 + x^3 + x + 1 \in K$ vorgegeben. Die Elemente von K lassen sich als Polynome in $\mathbb{F}_2[x]$ auffassen und haben Grad ≤ 7. Berechnen Sie das inverse Element von $g = x^7 + x^5 + x^2 + x + 1$, d.h. ein Element $g^{-1} \in \mathbb{F}_2[x]$ mit der Eigenschaft $g \cdot g^{-1} \equiv 1 \mod f$. Benutzen Sie dazu den erweiterten euklidischen Algorithmus. Schreiben Sie jeden Rechenschritt auf.

(iii) Sei $B := \{1, \zeta, \zeta^2, \ldots, \zeta^7\} \subseteq K$ eine Basis des $\mathbb{F}_2-$Vektorraumes K und $\alpha = \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 \in K$. Außerdem gilt $\zeta^8 + \zeta^4 + \zeta^3 + \zeta + 1 = 0$. Bestimmen Sie die Darstellende Matrix bzgl. der Basis B für die Abbildung

$$\phi : K \longrightarrow K, \quad x \longmapsto \alpha \cdot x.$$

2. Aufgabe **DES** **(5 Punkte)**

(i) Welche Auswirkung hat es, wenn man beim DES die Rundenschlüssel k_i in der umgekehrten Reihenfolge anwendet?

(ii) Das Bitkomplement sei mit $\bar{\cdot}$ bezeichnet. Also $\bar{1} = 0$ und $\bar{0} = 1$. Zeige $DES(\bar{m}, \bar{k}) = \overline{DES(m, k)}$.

(iii) Angenommen, es liegen ein paar Klartext-Chiffretext Paare vor und durch einen technischen Defekt eine Ein- und Ausgabe der ersten Runde von DES. Wie schwer ist es, den geheimen Schlüssel k zu berechnen?

3. Aufgabe **Polynomielle Algorithmen** **(3 Punkte)**

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 $k \geq k_0$.

(i) 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 eie 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.

(ii) 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.

(iii) 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.

4. Aufgabe **(8 Punkte)**

Praktische Aufgabe. Implementieren Sie entweder AES mit den Schlüssellängen 128, 192 und 256 oder DES in KASH3. Ver- und entschlüsseln Sie Ihre Matrikelnummern, die durch Anfügen von „F“s auf die richtige Blocklänge gebracht werden (d.h. verwenden Sie ihre Matrikelnummern sowohl als Klartext als auch als Chiffretext). Zur Hilfestellung gibt es ein paar vorprogrammierte Funktionen in der Datei AES.k auf der Webseite der VL. Für DES gibt es die Datei DES.k.

Hinweis: Die praktische Aufgabe kann bis zum 17.11.06 abgegeben werden.

Gesamt: 20 Punkte