Institut für Informatik
Algorithmen und Komplexität II
Prof. Dr. Johannes Köbler

WS 2002/3

Übungen zur Kryptologie II

9. Übung

Aufgabe 1

Zur Erinnerung: Bei der Lamport-Signatur wird ein Dokument $x = x_1 \cdots x_n \in \{0,1\}^n$ durch die Folge $y_{(i,x_i)}$, $i = 1, \ldots, n$ signiert, d.h. durch x wird aus der Grundmenge $A = \{1, \ldots, n\} \times \{0,1\}$ die Indexmenge $A_x = \{(i, x_i) \mid i = 1, \ldots, n\}$ ausgewählt.

a) Zeigen Sie, dass die Bedingung

$$x \neq x' \Rightarrow A_x \not\subseteq A_{x'}$$

notwendig für die Sicherheit der Lamport-Signatur ist.

b) Ein Mengensystem B_i, $i \in I$, heißt Spernersystem über B, falls gilt:

- $B_i \subseteq B$ für alle $i \in I$ und
- $i \neq j \Rightarrow B_i \not\subseteq B_j$.

Finden Sie für $B = \{1, \ldots, 2m\}$ ein Spernersystem B_i, $i \in I$, der Größe $\|I\| = \binom{2m}{m}$.

c) Benutzen Sie das Spernersystem aus Teilaufgabe b), um die Signaturlänge der Lamport-Signatur auf fast die Hälfte zu verkürzen.

d) Zeigen Sie, dass es kein Spernersystem der Größe $\|I\| > \binom{2m}{m}$ über $B = \{1, \ldots, 2m\}$ gibt.

Aufgabe 2 (4 Punkte)

Benutzen Sie das Chaum-van Antwerpen Verfahren mit den Parametern $p = 467$, $\alpha = 4$, $a = 101$ und $\beta = 449$, um eine verbindliche digitale Signatur für das Dokument $x = 64$ zu erzeugen. Zeigen Sie, wie Alice mit Hilfe des Abstreitungsprotokolls Bob davon überzeugen kann, dass eine ihr vorgelegte Signatur $y = 25$ für das Dokument $x = 157$ gefälscht ist (unter der Annahme, dass Bob die Zufallszahlen $e_1 = 46$, $e_2 = 123$, $f_1 = 198$ und $f_2 = 11$ benutzt).