Institut für Informatik
Komplexität und Kryptografie
Prof. Dr. Johannes Köbler

Sommersemester 2004

Übungen zur Kryptologie 2

7. Übung

Aufgabe 1

a) Falls sich bei der Berechnung einer ElGamal-Signatur (y, z) der Wert $z = 0$ ergibt, muss eine neue Zufallszahl k gewählt werden. Überlegen Sie, wie sich aus einer ElGamal-Signatur (y, z) mit $z = 0$ und dem öffentlichen Verifikationsschlüssel der geheime Signaturschlüssel berechnen lässt.

b) Beim DSA muss auch im Fall $y = 0$ eine neue Zufallszahl k gewählt werden. Überlegen Sie, wie sich aus einer DSA-„Signatur“ (y, z) mit $y = 0$ die benutzte Zufallszahl k bestimmt werden kann, und wie sich daraus für ein beliebiges Dokument x eine gefälschte „Signatur“ (y, z) mit $y = 0$ erhalten lässt.

c) Was würde es bedeuten, wenn man beim ECDSA-Signaturverfahren $y = 0$ oder $z = 0$ zulassen würde.

Aufgabe 2

a) Bestimmen Sie die NFA-Darstellung der Zahl 87.

b) Bestimmen Sie mit Hilfe des Algorithmus DoubleAddSub das Vielfache $87P$ des Punktes $P = (2, 6)$ auf der elliptischen Kurve E, die über $\mathbb{Z}_{127}$ durch $y^2 = x^3 + x + 26$ definiert ist.

Aufgabe 3

Wir bezeichnen mit L_i die Menge aller natürlichen Zahlen, die eine NAF-Darstellung der Form $(c_{i-1}, \ldots, c_0)$ mit $c_{i-1} = 1$ haben.

a) Zeigen Sie, dass die Anzahlen $l_i = \|L_i\|$ folgende Rekursionsgleichungen erfüllen:

$$\begin{aligned} l_1 &= 1, \\ l_2 &= 1, \\ l_{i+1} &= 2(l_1 + \cdots + l_{i-1}) + 1, i \geq 2. \end{aligned}$$

b) Finden Sie eine explizite Darstellung für l_i.

Aufgabe 4

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.