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

WS 2002/3

Übungen zur Kryptologie II

8. Übung

Aufgabe 1

a) Falls sich bei der Berechnung einer ElGamal-Signatur der Wert $z = 0$ ergibt, muss eine neue Zufallszahl r 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 r gewählt werden. Überlegen Sie, wie sich aus einer DSA-„Signatur" (y, z) mit $y = 0$ die benutzte Zufallszahl r 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 (4 Punkte)

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:

$$\begin{aligned} k_1 &= 1, \\ k_2 &= 1, \\ k_{i+1} &= 2(k_1 + \cdots k_{i-1}) + 1, i \geq 2. \end{aligned}$$

b) Finden Sie eine explizite Darstellung für k_i.