Übungen zur Kryptologie 2 Sommersemester 2008

Johannes Köbler/Sebastian Kuhnert

Übungsblatt 6

Aufgabe 43

Berechnen Sie den diskreten Logarithmus $\log_\alpha \beta$ in $\mathbb{Z}_p^*$ mit dem ρ-DLP-Algorithmus von Pollard für $p = 458009$, $\alpha = 2$ und $\beta = 56851$.

Hinweis: Die Ordnung von α in $\mathbb{Z}_p^*$ ist $n = 57251$. Benutzen Sie den Pseudozufallsgenerator aus der Vorlesung mit dem Startwert $x_0 = 1$.

Aufgabe 44

Sei A ein generischer DLP-Algorithmus für die Berechnung des diskreten Logarithmus $\log_\alpha \beta$ über der additiven Gruppe $\mathbb{Z}_{19}$, deren Elemente durch zufällig gewählte Bitstrings der Länge 5 kodiert sind. Wir nehmen an, dass A bei Eingabe $\alpha = 01100$ und $\beta = 10111$ zur Berechnung der Gruppenelemente $\alpha^c\beta^d$ die Orakelfragen (c, d) für alle Paare in der Menge

$$C = \{(1 - i^2 \bmod 19, i \bmod 19) \mid i = 0, 1, 2, 4, 7, 12\}$$

stellt.

a) Berechnen Sie *Good*(C).

b) Angenommen, A erhält folgende Orakelantworten:

$(1,0)$	$(0,1)$	$(16,2)$	$(4,4)$	$(9,7)$	$(9,12)$
01100	10111	00110	01010	00100	11001

Welche Information lässt sich hieraus über den Wert von $\log_\alpha \beta$ ableiten?

Aufgabe 45

Seien die Primzahl $p = 227$ und der Erzeuger $\alpha = 2$ von $\mathbb{Z}_p^*$ gegeben.

a) Berechnen Sie die Potenzen α^{32}, α^{40}, α^{59} und α^{156} in $\mathbb{Z}_p^*$ und faktorisieren Sie diese über der Faktorbasis $B = \{2, 3, 5, 7, 11\}$.

b) Bestimmen Sie die diskreten Logarithmen $\log_\alpha p$ der Basisprimzahlen $p \in B$.

c) Berechnen Sie $\log_\alpha \beta$ für $\beta = 173$ mit der Index-Calculus Methode.

Hinweis: Benutzen Sie die Faktorbasis B und die Zufallszahl 177.

Aufgabe 46

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

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

Aufgabe 47

Die Punkte der *projektiven Ebene* werden durch die Ursprungsgeraden

$$g(X, Y, Z) = \{(\lambda X, \lambda Y, \lambda Z) \mid \lambda \in \mathbb{R}\},\ (X, Y, Z) \in \mathbb{R}^3 - \{(0, 0, 0)\}$$

gebildet. Es gilt also $g(X, Y, Z) = g(X', Y', Z')$, falls ein $\lambda \in \mathbb{R} - \{0\}$ existiert mit $X' = \lambda X$, $Y' = \lambda Y$ und $Z' = \lambda Z$.

a) Überlegen Sie, wie sich die affine Ebene $\mathbb{R}^2$ in die projektive Ebene einbetten lässt. *Hinweis:* Verwenden Sie nur projektive Punkte der Form $g(X, Y, 1)$.

b) Zeigen Sie, dass von dieser Einbettung genau die projektiven Punkte der Form $g(X, Y, 0)$ nicht erfasst werden. Welche Punkte müsste man zum $\mathbb{R}^2$ hinzunehmen, damit diese Einbettung zu einem Isomorphismus wird? Geben Sie eine geometrische Interpretation dieser Punkte.

c) Im $\mathbb{R}^2$ sei eine Kurve durch eine Gleichung der Form $F(x, y) = y^2 - x^3 - ax - b = 0$ definiert. Wie lässt sich hieraus eine Kurvengleichung $\tilde{F}(X, Y, Z) = 0$ für die Einbettung $\{g(x, y, 1) \mid F(x, y) = 0\}$ dieser Kurve in die projektive Ebene gewinnen?

d) Welche projektiven Punkte der Form $g(X, Y, 0)$ erfüllen ebenfalls die Gleichung $\tilde{F}(X, Y, Z) = 0$?

Aufgabe 48 (10 Punkte)

Betrachten Sie die mittels

$$y^2 = x^3 - 3x - 2$$

über den reellen Zahlen definierte elliptische Kurve E.

a) Skizieren Sie zeichnerisch den Verlauf von E.

b) Berechnen Sie die Summe $P + Q$ für $P = (3, 4)$ und $Q = (2, 0)$.

c) Berechnen Sie die Punkte $2P = P + P$ und $2Q = Q + Q$.