Übungen zur Vorlesung Kryptographie

Blatt 9

Aufgabe 33: (Aufwärmübung zu elliptischen Kurven)
Lösen Sie diese Aufgabe nur per Hand, also ohne jede Computerhilfe.

(a) Zeigen Sie, dass die Gleichung $y^2 = x^3+3x+1$ eine elliptische Kurve E über $\mathbb{F}_{11}$ definiert.
(b) Welche der Punkte $p = (2, 3)$, $q = (3, -2)$ und $r = (4, 0)$ sind Elemente von E?
(c) Was sind jeweils die inversen Elemente von $p = (5, 3)$, $q = (2, 9)$ und $r = (4, 0)$ in E?
(d) Berechnen Sie $(4, 0) \odot (1, 4)$, $(5, 3) \odot (0, 1)$ und $(0, 1) \odot (5, 3)$ in E.
(e) Berechnen Sie p^2 für $p = (1, 4)$.

Aufgabe 34: (Diffie-Hellman auf elliptischen Kurven)
Hier führen Sie den Diffie-Hellman-Schlüsseltausch auf einer konkreten (unrealistisch kleinen) elliptischen Kurve durch. Es sei E^* die elliptische Kurve, die durch $y^2 = x^3 + x$ über $\mathbb{F}_7$ gegeben ist.
(Es ist hilfreich, den Cayleygraphen die Gruppe E^* aus Bsp. 6.2 des Skripts zu nutzen: damit kann praktisch alles hier ohne Formeln berechnet werden.)

(a) Ein Erzeuger von E^* ist $g = (3, 3)$. Die öffentliche Information ist (E^*, g). Alice geheimer Schlüssel ist $a = 5$, Bobs geheimer Schlüssel ist $b = 3$. Was schickt Alice an Bob? Was schickt Bob an Alice? Was ist ihr gemeinsamer Schlüssel k?

(b) Ein anderer Erzeuger von E^* ist $g' = g^3 = (5, 5)$. Die öffentliche Information ist jetzt (E^*, g'). Alice geheimer Schlüssel ist wieder $a = 5$, Bobs geheimer Schlüssel ist wieder $b = 3$. Was schickt Alice diesmal an Bob? Was schickt Bob diesmal an Alice? Was ist ihr gemeinsamer Schlüssel k?

Aufgabe 35: (Wann ist's keine Gruppe?)
(a) Es wäre nahliegend, die Gruppenoperation auf einer elliptischen Kurve E über $\mathbb{R}$ einfach zu definieren als $p \odot q = r$, wobei r der dritte Schnittpunkt der Gerade durch p und q mit E ist (bzw der zweite Schnittpunkt von E mit der Tangente in p an E, falls $p = q$). Erklären Sie, warum das im Allgemeinen keine Gruppe liefert. Welche Gruppenaxiome werden verletzt? Gerne kann Ihre Lösung durch ein aussagekräftiges Bild illustriert werden.

(b) Für welche Werte von b liefert $y^2 = x^3 + b$ keine elliptische Kurve über $\mathbb{R}$? Für welche Werte von b liefert $y^2 = x^3 - 3x + b$ keine elliptische Kurve über $\mathbb{R}$? Zeichnen Sie all diese Kurven (gerne mit einer geeigneten Software). Erläutern Sie, warum die jeweils keine Gruppe liefern.

Aufgabe 36: (Ordnung von E ist ungefähr p)
Sei E eine elliptische Kurve über $\mathbb{F}_p$ (wie in Def. 6.1).

(a) Zeigen Sie, dass E spiegelsymmetrisch bezüglich der x-Achse ist. (Also: ist $(x, y) \in E$, dann auch $(x, -y) \in E$. Das $\mathcal{O}$ kann hier ignoriert werden.)

(b) Zeigen Sie, dass E spiegelsymmetrisch bezüglich der Achse $\{(x, \frac{p}{2}) \mid x \in \mathbb{R}\}$ ist.
(Zwar ist $\frac{p}{2}$ nicht in E oder $\mathbb{F}_p$, aber das Spiegeln haut dennoch hin.)

(c) Zeigen Sie: für die Ordnung $|E|$ von E gilt: $|E| \leq 2p + 1$.

Abgabe bis Dienstag 18.6.2024 bis 23:59 Uhr per Email an den Tutor.

Jakob Niermann	Mi 16 Uhr in T2-233	janiermann+krypto@techfak.de
Enrico di Gaspero	~~Do 16 Uhr in U2-216~~	edigaspero+krypto@techfak.de
Lisa Henetmayr	Fr 10 Uhr in X-E0-205	lhenetmayr+krypto@techfak.de
Richard Freidhof	Fr 12 Uhr in T2-141	rfreidhof+krypto@techfak.de