Dr. Dirk Frettlöh 10.6.2026

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 naheliegend, 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.

(Fortsetzung auf Seite 2)

Aufgabe 36: (Elemente der Ordnung 3)

Recall: ein Element g in einer Gruppe G hat Ordnung k, falls $g^k = e$ ist (e das neutrale Element), und für alle $i \in \{1, \ldots, k-1\}$ gilt $g^i \neq e$.
Für ein Element g einer Gruppe G bezeichnen wir die Ordnung von g mit $o(g)$.

(a) Sei $G \times H$ das direkte Produkt zweier Gruppen und sei $(g, h) \in G \times H$. Zeigen sie, dass gilt

$$o((g, h)) = \text{kgV}(o(g), o(h)).$$

Dabei bezeichnet $o(g)$ die Ordnung von g in G und $o(h)$ die Ordnung von h in H, und kgV steht für das kleinste gemeinsame Vielfache.

(b) Was sind die möglichen Anzahlen an Elementen von Ordnung 3, die eine elliptische Kurve E über $\mathbb{F}_p$ haben kann. Begründen Sie ihre Antwort. (*Tipp: Es gibt drei unterschiedliche möglichen Anzahlen, also E hat entweder x_1 oder x_2 oder x_3 Elemente von Ordnung 3. Sie müssen $\{x_1, x_2, x_3\}$ bestimmen.*)

(c) Bestimmen Sie für die folgenden elliptischen Kurven alle Elemente der Ordnung 3 und begründen Sie, warum das alle sind.

- $E_1 : y^2 = x^3 + x + 2$ über $\mathbb{F}_{13}$
- $E_2 : y^2 = x^3 + 7x$ über $\mathbb{F}_{13}$
- $E_3 : y^2 = x^3 + 3x + 2$ über $\mathbb{F}_{11}$

Abgabe bis Mittwoch 17.6.2026 bis 12:00 Uhr per Email an die Tutorin.

Lisa Henetmayr Mi 12 Uhr in S0-115 lhenetmayr+krypto@techfak.de
Lisa Henetmayr Mi 16 Uhr in U2-147 lhenetmayr+krypto@techfak.de