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 nun ihr gemeinsamer Schlüssel k?

Aufgabe 35: (Three-Pass-Protokoll auf elliptischen Kurven)
Bob möchte die Nachricht 6 an Alice schicken und dabei Shamirs Three-Pass-Protokoll über der elliptischen Kurve E mit der Gleichung $y^2 = x^3 + 3x + 2$ über $\mathbb{F}_{11}$ nutzen. Der öffentliche Erzeuger von E sei $g = (3, 7)$. Alice' geheimer Schlüssel ist $a = 3$, Bobs geheimer Schlüssel ist $b = 4$. Bob kodiert die 6 als $m = (6, 7)$ in E.

Was sind die Werte von a' und b'? Und was genau schicken Bob und Alice sich gegenseitig?

(Es ist sicher auch hier hilfreich, den Cayleygraphen von E zu erstellen und zu nutzen.)

Aufgabe 36: (Elemente der Ordnung 2)
Erinnerung: 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: $g^i \neq e$.

(a) Bestimmen Sie jeweils alle Elemente der Ordnung zwei in den beiden Gruppen E und E^* in Beispiel 6.2 des Skripts.

(b) Zeigen Sie, dass eine elliptische Kurve als Gruppe maximal drei Elemente der Ordnung zwei hat.

(Ein plausibles Bild über $\mathbb{R}$ gibt bereits Teilpunkte, ein formales Argument gibt volle Punktzahl.)

Abgabe bis Mittwoch 10.6.2020 bis 14 Uhr per Email an den Tutor.

Philipp Braukmann pbraukmann@techfak.de
Jonas Friemel jfriemel+krypto@techfak.de