Übungen zur Vorlesung Kryptographie

Blatt 10

(Es ist in A37-38 hilfreich, jeweils den Cayleygraphen der Gruppe E zu nutzen. Den können Sie sich mit der Software auf der Webseite zur Vorlesung besorgen.)

Aufgabe 37: (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 $y^2 = x^3 + x + 5$ über $\mathbb{F}_{11}$ gegeben ist.

(a) Ein Erzeuger von E ist $g = (2, 2)$. Die öffentliche Information ist (E, g) . Alices 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 $g' = g^7 = (7, 6)$. Die öffentliche Information ist jetzt (E, g') . Alices 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 38: (ElGamal auf elliptischen Kurven)

Hier führen Sie die ElGamal-Verschlüsselung auf einer konkreten elliptischen Kurve durch.

Angenommen, Bob möchte eine Nachricht an Alice schicken und dabei ElGamal über der elliptischen Kurve E^* mit der Gleichung $y^2 = x^3 + x$ über $\mathbb{F}_{11}$ nutzen. Der öffentliche Erzeuger von E^* sei $g = (8, 5)$. Alices geheimer Schlüssel ist $a = 3$.

(a) Was ist das g^a in Alice' öffentlichem Schlüssel (E^*, g, g^a) ?

(b) Bob wählt zufällig $r = 2$. Was ist der Einmalschlüssel $k = (g^a)^r$ für diese Verschlüsselung?

(c) Bob verschlüsselt die Nachricht $m = 5$. Dazu wählt er das Element $(5, 3) \in E^*$ und verschlüsselt es als $c = m \odot k$. Was ist c ? Was genau schickt Bob an Alice?

(d) Was berechnet Alice alles, um die Nachricht zu entschlüsseln?

Aufgabe 39: (Gruppenstruktur)

Eine elliptische Kurve hat — als abstrakte Gruppe — immer die Struktur einer zyklischen Gruppe Z_n , oder des direkten Produkts $Z_k \times Z_\ell$ zweier zyklischer Gruppen Z_k und Z_ℓ .

Bestimmen Sie die Struktur der elliptischen Kurven (als Gruppen), die durch die Gleichungen $y^2 = x^3 + ax$ für $a = 1, 2, 3$ über $\mathbb{F}_{17}$ gegeben sind (*dazu ist die Software von meiner Webseite sehr hilfreich!*) und zeichnen Sie jeweils ihren Cayleygraphen.

Aufgabe 40: (Buchstaben zu Punkten zu Buchstaben)

Wir benutzen die Koblitz-Kodierung aus der Vorlesung für die elliptische Kurve mit der Gleichung $y^2 = x^3 + x + 3$ über $\mathbb{F}_{17}$. Dabei ist wie üblich $a=0, b=1, \dots, z=25$. Also können wir jeden Buchstaben mit 6 Bit darstellen. Wir wählen hier also $d = 4$ und zerschneiden eine zu verschlüsselnde Botschaft (in Binärcodierung) in 2-Bit-Worte.

(a) Berechnen Sie die Koblitz-Kodierung des Buchstaben "t". Zeigen Sie Ihre Berechnung.

(b) Welches Wort ergibt das Ent-Kodieren der nach obigem Schema Koblitz-kodierten Nachricht

(6, 2), (2, 8), (8, 8), (2, 9), (7, 8), (12, 3), (3, 4), (2, 8), (3, 13), (2, 9), (12, 3), (2, 9), (3, 4), (12, 14), (2, 8), (7, 8), (3, 13), (7, 9)?

Abgabe bis Mittwoch 18.6.2025 bis 14 Uhr per Email an die Tutorin.

Lisa Harms lharms+krypto@techfak.de
 Lisa Henetmayr lhenetmayr+krypto@techfak.de