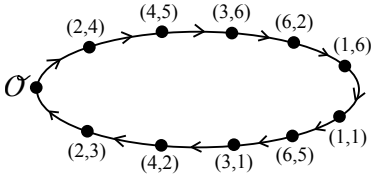
Dr. Dirk Frettlöh 17.6.2026

Übungen zur Vorlesung Kryptographie

Blatt 10

Aufgabe 37: (dlog in elliptischen Kurven)

(a) Rechts ist der Cayleygraph der elliptischen Kurve E über $\mathbb{F}_7$ mit $y^2 = x^3 + x + 6$ gezeigt, bezüglich des Erzeugers $g = (2, 4)$. Ermitteln Sie mittels des Graphen $\mathrm{dlog}_g((3, 6))$, $\mathrm{dlog}_g((6, 5))$, $\mathrm{dlog}_{(3,6)}((1, 1))$, $\mathrm{dlog}_{(3,6)}((6, 2))$ und $\mathrm{dlog}_{(4,2)}(g)$. Geben Sie eine kurze Begründung, die Zahlen reichen allein nicht.



(b) Existiert in der elliptischen Kurve E aus (a) der $\mathrm{dlog}_p(q)$ für alle $p, q \in E \setminus \mathcal{O}$? Existiert in der elliptischen Kurve E' über $\mathbb{F}_7$ mit der Gleichung $y^2 = x^3 + 3x + 1$ $\mathrm{dlog}_p(q)$ für alle $p, q \in E' \setminus \mathcal{O}$? Begründen Sie Ihre Antworten.

Aufgabe 38: (ElGamal auf elliptischen Kurven)

Bob möchte eine Nachricht an Alice schicken und dabei ElGamal-Verschlüsselung 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 $a = 3$.

(a) Was ist das g^a in Alice öffentlichem Schlüssel (E, g, g^a)?
(b) Bob wählt zufällig $r = 6$. Was ist der Einmalschlüssel $k = (g^a)^r$ für diese Verschlüsselung?
(c) Bob verschlüsselt die Nachricht $m = 10$. Dazu wählt er das Element $(10, 3) \in E$ 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?

(Es ist vermutlich auch hier hilfreich, den Cayleygraphen zu haben und zu nutzen. Dazu und für andere Aufgaben auf diesem Blatt ist die Software von meiner Webseite sicher wieder hilfreich.)

Aufgabe 39: (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, ... 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

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

Aufgabe 40: (Polynome über $\mathbb{F}_2$ - Level 1 bis 3)

Wir betrachten Polynome in $\mathbb{F}_2[x]$, also Polynome von der Form $a_n x^n + \cdots + a_1 x + a_0$ mit $a_i \in \mathbb{F}_2$ für $0 \le i \le n$.

(a) Berechnen Sie in $\mathbb{F}_2[x]$ die Ergebnisse von $(x^8+x^7+x^5+x^4+x^2+1)+(x^8+x^6+x^4+x^3+x^2+x+1)$ und $(x^4 + x^2 + 1) \cdot (x^3 + x + 1)$.
(b) Sei $p = x^5 + x^4 + x + 1$. Berechnen Sie $p \bmod x^4 + x^2$, $p \bmod x^4 + x$, und $p \bmod x^4 + 1$ in $\mathbb{F}_2[x]$.
(c) Berechnen Sie den ggT von $x^3 + 1$ und $x^4 + x^2 + x + 1$ in $\mathbb{F}_2[x]$.

(Tipp: Benutzen Sie bei (c) den euklidischen Algorithmus, angepasst an Polynome über $\mathbb{F}_2$, vgl. Beispiel aus der Vorlesung, oder auch Beispiel 8.1 im Skript S. 47.)

Abgabe bis Mittwoch 24.6.2026 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