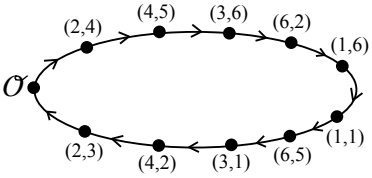
# Übungen zur Vorlesung Kryptographie

## 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: (Buchstaben zu Punkten zu Buchstaben)**

Wir benutzen die Koblitz-Kodierung aus der Vorlesung für die elliptische Kurve $E$ mit der Gleichung $y^2 = x^3 + 5x + 3$ 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)** Was ist die Koblitz-Kodierung des Buchstaben "y"?

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

$$(1, 3), (13, 2), (4, 6),\ (1, 3), (10, 13), (1, 14),\ (5, 0), (2, 2), (10, 13),\ (4, -6), (2, -2), (15, -6)?$$

**(c)** Finden Sie ein $b$, so dass die Koblitz-Kodierung mit $d = 4$ für die elliptische Kurve $E$ mit der Gleichung $y^2 = x^3 + 5x + b$ über $\mathbb{F}_{17}$ versagt. (D.h., es gibt ein $m \in \{0, 1, 2, 3\}$, so dass für kein $x = dm + j$ ($j \in \{0, 1, 2, 3\}$) ein $y$ existiert mit $(x, y) \in E$.)

**Aufgabe 39: (Gruppenstruktur)**

Bestimmen Sie — im Sinne von Satz 6.1 — die Struktur der elliptischen Kurven, die durch die Gleichungen $y^2 = x^3 + ax$ für $a = 1, 2, 3$ über $\mathbb{F}_{17}$ gegeben sind und zeichnen Sie jeweils ihren Cayleygraphen. *(Als Lösung reicht der Graph mit Knoten und Kanten, die Knoten brauchen nicht beschriftet zu werden.)*

**Aufgabe 40: (Einfache Hashfunktion)**

Wir codieren Buchstaben als $a = 00, b = 01, c = 02 \ldots, z = 25$. Wir benutzen eine Merkle-Damgård-Konstruktion mit Startwert $s = x_0 = 73$. Die $m_i$ sind die einzelnen Buchstaben $m_1, m_2, \ldots, m_n$ des zu hashenden Texts, gefolgt von der Länge $m_{n+1} := n$ der Nachricht; also $m = (m_1, m_2, \ldots, m_n, m_{n+1} = n)$, als zweistellige Zahlen gelesen. Die Kompressionsfunktion $x_i = f(x_{i-1}, m_i)$ ($i = 1, \ldots, n + 1$) funktioniert folgendermaßen:

(1) $y = 19 \cdot (m_i + x_{i-1}) \bmod 100$
(2) Vertausche die Ziffern von $y$, nenne diese neue Zahl $z$ (Obacht: aus $y = 7 = 07$ wird 70)
(3) $x_i = x_{i-1} + z \bmod 100$

Was ist der Hashwert $h(m)$ des Wortes $m =$"passwort"? Finden Sie ein (sinnfreies) Wort mit demselben Hashwert $h(m)$. Was ist der Hashwert von $m' =$"a"? Was ist der Hashwert von $m'' =$"password"? Was ist der Hashwert des leeren Strings ""?

---

**Abgabe** bis Dienstag 25.6.2024 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 |