

Übungen zur Vorlesung Kryptographie

Blatt 8

Aufgabe 29: (ElGamal mod p)

Der öffentliche ElGamal-Schlüssel von Alice ist $(G, g, g^a) = (Z_{67}^*, 2, 18)$.

(a) Was berechnet Bob, um die Nachricht $m = 11$ mit der Zufallszahl $r = 7$ zu verschlüsseln? Was sendet er genau an Alice?

(b) Was berechnet Alice, um die Nachricht $(c, g^r) = (32, 17)$ zu entschlüsseln?

(c) Was ist Alices geheimer Schlüssel a ? Und welches r hat Bob in Teil (b) gewählt?

(Teil (c) geht natürlich nur, weil die hier verwendeten Zahlen unrealistisch klein sind.)

Aufgabe 30: (Eve vs Shamirs Three-Pass-Protokoll)

Zeigen Sie, dass Shamirs Three-Pass-Protokoll mit $G = Z_p^*$ höchstens so schwierig zu knacken ist wie das Berechnen des diskreten Logarithmus mod p . Genauer: Angenommen, Eve entwickelt eine Methode, den diskreten Logarithmus $\text{dlog}_g(x) \bmod p$ effizient zu berechnen. Zeigen Sie, dass sie dann aus m^a, m^{ab} und $m^{ba'}$ die Nachricht m berechnen kann.

(Tipp: was ist $\text{dlog}_{m^{ab}}(m^a)$?)

Aufgabe 31: (Quadriken)

Bestimmen Sie die Typen der folgenden Quadriken. Sie dürfen sie einfach von einem Rechner bzw einer Webseite bzw einer App zeichnen lassen und so auf den Typ schließen.

$$Q_1 = \{(x, y) \in \mathbb{R}^2 \mid y^2 - x^2 + xy - 1 = 0\}, \quad Q_2 = \{(x, y) \in \mathbb{R}^2 \mid y^2 + x^2 + xy - 1 = 0\}$$

$$Q_3 = \{(x, y) \in \mathbb{R}^2 \mid y^2 - x^2 + xy = 0\}, \quad Q_4 = \{(x, y) \in \mathbb{R}^2 \mid y^2 - x - y - 1 = 0\}$$

Eine der Quadriken ist eine Parabel. Begründen Sie für diese genau, warum es nichts anderes sein kann.

Aufgabe 32: (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 $y^2 = x^3 - 3x + b$ keine elliptische Kurve über $\mathbb{R}$? Für welche Werte von b liefert $y^2 = x^3 + b$ keine elliptische Kurve über $\mathbb{R}$? Zeichnen Sie all diese Kurven (gerne mit einer geeigneten Software). Erläutern Sie, warum die jeweils keine Gruppe liefern.

Abgabe bis Mittwoch 3.6.2020 bis 14 Uhr per Email an den Tutor.