

Übungen zur Vorlesung Kryptographie

## Blatt 8

**Aufgabe 29: (Wieviele dlogs?)**

(a) Finden Sie drei Primzahlen  $a, b, p \in \mathbb{N}$  mit  $1 < a < p$ ,  $1 < b < p$ ,  $a \neq b$ , so dass  $\text{dlog}_a(b)$  modulo  $p$  nicht existiert.

(b) Sei  $g$  ein Erzeuger von  $G$ . Zeigen Sie, dass für jedes  $a \in G$  der diskrete Logarithmus  $\text{dlog}_g(a)$  existiert.

(c) Sei nun  $|G|$  gerade und  $g$  kein Erzeuger von  $G$ , sondern  $g$  habe die Ordnung  $|G|/2$ . Wieviel Werte kann der diskrete Logarithmus  $\text{dlog}_g(a)$  für ein  $a \in G$  annehmen? Begründen Sie Ihre Antwort.

**Aufgabe 30: (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? Welche Werte sendet er genau an Alice?

(b) Was ist Alice geheimer Schlüssel  $a$ ?

(c) Was berechnet Alice, um die Nachricht  $(c, g^r) = (31, 17)$  mittels des  $a$  aus Teil (b) zu entschlüsseln?

(d) Nun schickt Bob  $(c, g^r) = (17, 37)$ . Welches  $r$  hat Bob gewählt?

*(Teil (b) und (d) gehen natürlich nur, weil die hier verwendeten Zahlen unrealistisch klein sind.)*

**Aufgabe 31: (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  $m^{aba'}$  die Nachricht  $m$  berechnen kann.

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

**Aufgabe 32: (Quadriken)**

(a) 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.

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

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

(b) Eine der Quadriken ist ein Paar sich kreuzender Geraden. Begründen Sie für diese mathematisch genau, warum es nichts anderes sein kann.

**Abgabe** bis Dienstag 11.6.2024 bis 23:59 Uhr per Email an den Tutor.

|                   |                                |                              |
|-------------------|--------------------------------|------------------------------|
| Jakob Niermann    | Mi 16 Uhr in T2-233            | janiermann+krypto@techfak.de |
| Enrico di Gaspero | <del>Do 16 Uhr in U2-216</del> | 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  |