# Übungen zur Vorlesung Kryptographie

## Blatt 8

**Aufgabe 29: (Primitivwurzeln für Diffie-Hellman finden)**
Wir betrachten einen Diffie-Hellman-Schlüsseltausch mit $G = Z_p^*$ mit $p$ Primzahl. Im Allgemeinen ist es knifflig, eine echte Primitivwurzel mod $p$ zu finden. Folgende Idee hilft: Finde eine Primzahl $q$ einer gewünschten Länge $n$ (sagen wir, 1024 bit), so dass auch $p = 2q + 1$ Primzahl ist. (Das geht in $O(n^2)$ statt in $O(n)$ Versuchen.)

**(a)** Bestimmen Sie alle Werte $i \in \{1, \ldots, p-1\}$, so dass es ein $a \in Z_p^*$ gibt mit $a^i \equiv 1 \bmod p$, und $a^j \not\equiv 1 \bmod p$ für alle $j \in \mathbb{N}$ mit $1 \leq j < i$.

**(b)** Bestimmen Sie für die beiden kleinsten dieser Werte $i$ alle $a \in Z_p^*$ mit $a^i \equiv 1 \bmod p$.

**(c)** Wie kann Alice nun schnell eine Primitivwurzel mod $p$ finden?

**Aufgabe 30: (ElGamal mod p)**
**(a)** Der öffentliche Schlüssel von Alice ist $(p, g, g^a \bmod p) = (601, 7, 598)$. Verschlüsseln Sie die Nachricht $m = 12$ an Alice. Benutzen Sie dabei $r = 3$ als Zufallszahl.

**(b)** Der öffentliche Schlüssel von Alice sei wie in (a), der private Schlüssel sei $a = 4$. Entschlüsseln Sie die Nachricht $(g^r \bmod p, c) = (15, 13)$.

**(c)** Angenommen, Bob wählt zweimal denselben Exponenten $r$ und berechnet damit aus den Klartexten $m = 23$ und $m'$ jeweils die Schlüsseltexte $(57, 466)$ und $(57, 459)$, wobei $(601, 7, 21)$ der öffentliche Schlüssel von Alice ist. Berechnen Sie den Klartext $m'$.

**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.

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

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

**Bonusfrage:** *(für einen Extrapunkt)* Eine der Quadriken ist ein Paar sich kreuzender Geraden. Begründen Sie für diese genau, warum es nichts anderes sein kann.

**Aufgabe 32: (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 $\mathrm{dlog}_g(x) \bmod p$ effizient zu berechnen. Zeigen Sie, dass sie dann aus $m^a, m^{ab}$ und $m^{aba'}$ die Nachricht $m$ berechnen kann.

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

---

**Abgabe** bis Montag 13.6.2022 bis 14 Uhr per Email an Ihren Tutor.
Bitte auf jeder Abgabe das Tutorium angeben. Bitte die Abgaben so nennen: *techfakaccount*-bl$n$.pdf, also z.B. `dfrettloeh-bl8.pdf`, oder `dfrettloeh+mnebel-bl8.pdf`.

Jan-Philipp Brünger jbruenger@techfak.de
Simon Hahm shahm+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de