Übungen zur Vorlesung Kryptographie

Blatt 8

Aufgabe 29: (ElGamal mod p)
Wiur betrachten die ElGamal-Verschlüsselung aus der Vorlesung. Der öffentliche ElGamal-Schlüssel von Alice ist $(G, g, g^a) = (Z_{101}^*, 3, 38)$.

(a) Was berechnet Bob, um die Nachricht $m = 42$ mit der Zufallszahl $r = 17$ zu verschlüsseln? Was sendet er genau an Alice?

(b) Was berechnet Alice, um die Nachricht $(c, g^r) = (31, 31)$ 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: (Schmidt-Samoa-Verschlüsselung)
Es gibt neben ElGamal und RSA erstaunlich wenige andere Private-Key-Verschlüsselungsverfahren. Hier sollen Sie eines untersuchen.

Vorab: Alice wählt zwei große Primzahlen p, q und berechnet $N = p^2q$. Außerdem berechnet Sie $d \equiv N^{-1} \bmod R$, wobei R das kleinste gemeinsame Vielfache von $p-1$ und $q-1$ ist.

N ist der öffentliche Schlüssel, p, q, R und d sind geheim.

Verschlüsseln: Bob wählt ein m mit $0 \le m < pq$ und sendet $c \equiv m^N \bmod N$ an Alice.

Entschlüsseln: Alice berechnet m als $m \equiv c^d \bmod pq$.

(a) Zeigen Sie, dass das Verfahren korrekt ist.

(b) N ist ja viel größer als pq. Warum die Einschränkung "m mit $0 \le m < pq$"?

(c) Worauf beruht die Sicherheit dieses Verfahrens? (Also, was müsste Eve können, um das Verfahren zu knacken?)

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.

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

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

Eine der Quadriken ist eine Parabel, eine andere ist ein Paar sich kreuzender Geraden. Begründen Sie für diese beiden genau, warum es nichts anderes sein kann. (Warum z.B. ist jenes, das wie eine Parabel aussieht, nicht doch eine sehr lange Ellipse?)

Aufgabe 32: (Wann ist's keine Gruppe?)
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 9.6.2021 bis 14 Uhr per Email an den

Tutor. Jan Jan-Philipp Brünger jbruenger@techfak.de
Leonard Simon Ellinghaus lellinghaus+krypto@techfak.de
Kallias Stoupas kstoupas+krypto@techfak.de