Dr. Dirk Frettlöh 24.5.2023

Übungen zur Vorlesung Kryptographie

Blatt 8

Aufgabe 29: (ElGamal mod p)
Der öffentliche ElGamal-Schlüssel von Alice ist $(G, g, g^a) = (Z_{101}^*, 2, 18)$.

(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 $(c, g^r) = (23, 27)$ zu entschlüsseln?

(d) Nun schickt Bob $(c, g^r) = (77, 37)$. Welches r hat Bob gewählt?

(Teil (b) und (d) gehen 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 $\mathrm{dlog}_g(x)$ mod 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 $\mathrm{dlog}_{m^{ab}}(m^a)$*?)*

Aufgabe 31: (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 32: (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 mathematisch genau, warum es nichts anderes sein kann.

Abgabe bis Dienstag 30.5.2023 bis 23:59 Uhr per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben!

Jakob Niermann janiermann+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de