Kryptographie - Algebraischer Hintergrund
Prof . Dr. F.-O. Schreyer
Übungsblatt 4: Elliptische Kurven Kryptogrphie

Abgabetermin 28.5.2002
Voraussetzungen: Vorlesungskapitel Public-Key-Kryptographie, Elliptische Kurven.

1. Das ElGamal-Kryptosystem funktioniert wie folgt:

   Bob wählt eine Primzahl p und ein $g \in \mathbb{F}_p^*$ mit $\mathbb{F}_p^* = \langle g \rangle := \left\{ g^k \mid k = 0, ..., p-1 \right\}$.

   Dann wählt er ein zufälliges $d \in \{1, ...p-2\}$, welches er geheim hält.

   Der öffentliche Schlüssel ist $g^d \in \mathbb{F}_p^*$ zusammen mit g und p.

   Alice kann nun eine für Bob bestimmte Nachricht $T \in \mathbb{F}_p^*$ wie folgt verschlüsseln:

   Alice wählt ein zufälliges $k \in \{1, ...p-2\}$ und berechnet

   $$\left(g^k, T \cdot \left(g^d \right)^k \right)$$

   Alice schickt dies an Bob und dieser berechnet

   $$\left(g^k \right)^d = \left(g^d \right)^k$$

   und bekommt damit wieder den Klartext

   $$T = \left(T \cdot \left(g^d \right)^k \right) \cdot \left(\left(g^d \right)^k \right)^{-1}$$

   Kann man $d = \log_g \left(g^d \right)$ berechnen, dann hat man das System geknackt.

   (a) Schreiben Sie eine Maple-Prozedur mit dem Alice eine Nachricht für Bob mit dem ElGamal-Kryptosystem verschlüsseln kann.

   (b) Schreiben Sie eine Maple-Prozedur mit der Bob diese Nachricht wieder entschlüsseln kann.

   (c) Schreiben Sie eine Maple-Prozedur, die das ElGamal-Kryptosystem knackt, indem sie aus dem öffentlichen Schlüssel den geheimen Schlüssel berechnet.

   (d) Probieren Sie Ihre Skripte mit einem frei gewählten Beispiel aus.

   Bem: Das Kodieren und Dekodieren der Nachricht als Zahl soll wie im RSA Skript durchgeführt werden.

2. Im ElGamal-Kryptosystem kann man $\mathbb{F}_p^*$ auch durch eine elliptische Kurve über einem endlichen Körper ersetzen:

   Bob wählt eine Primzahl p und eine elliptische Kurve $E(\mathbb{F}_p)$ über $\mathbb{F}_p$ und einen Punkt $g \in E(\mathbb{F}_p)$.

   Sei $H := \langle g \rangle$ die von g erzeugte zyklische Untergruppe von $E(\mathbb{F}_p)$.

   Dann wählt er ein zufälliges $d \in \{1, \ldots |H| - 1\}$, welches er geheim hält.

   Der öffentliche Schlüssel ist $d \cdot g$ zusammen mit g und $E(\mathbb{F}_p)$.

   Alice kann nun eine für Bob bestimmte Nachricht $T \in E(\mathbb{F}_p)$ wie folgt verschlüsseln:

   Alice wählt ein zufälliges $k \in \{1, \ldots |H| - 1\}$ und berechnet

   $$(k \cdot g, T + k \cdot (d \cdot g))$$

   Alice schickt dies an Bob und dieser berechnet

   $$d \cdot (k \cdot g) = k \cdot (d \cdot g)$$

   und bekommt damit wieder den Klartext

   $$T = (T + k \cdot (d \cdot g)) - k \cdot (d \cdot g)$$

   (a) Schreiben Sie eine Maple-Prozedur, mit der Alice eine Nachricht für Bob mit dem elliptischen Kurven ElGamal Kryptosystem verschlüsseln kann.

   (b) Schreiben Sie eine Maple-Prozedur, mit der Bob diese Nachricht wieder entschlüsseln kann.

   (c) Probieren Sie Ihr Skript mit der elliptischen Kurve $E : y^2 = x^3 + x + 1$ über $\mathbb{Z}/5\mathbb{Z}$ mit einem beliebigen Punkt g und einem Punkt der Kurve als Nachricht aus.

   (d) Haben Sie eine Idee, wie man auf elliptischen Kurven den log berechnen und damit ElGamal knacken kann.

Abgabe der Aufgaben bitte als email an

boehm@btm8x5.mat.uni-bayreuth.de
oder
boehm@math.uni-sb.de