Kryptographie - Algebraischer Hintergrund

Prof . Dr. F.-O. Schreyer

Übungsblatt 5: Endliche Körper und Quadratische Reziprozität

Abgabetermin 18.6.2002

Voraussetzungen: Vorlesungskapitel Endliche Körper, Quadratische Reziprodizität.

1. Schreiben Sie ein Maple-Skript, das die Anzahl der irreduziblen Polynome vom Grad r in $\mathbb{F}_p[x]$ bestimmt.

2. Schreiben Sie ein Maple-Skript, das für $q = p^r$ den Körper $\mathbb{F}_q \simeq \mathbb{F}_p[x]/(f)$ mit einem irreduziblen Polynom $f \in \mathbb{F}_p[x]$ vom Grad r konstruiert, d.h. Multiplikation, Addition und Bildung des Inversen realisiert auf Repräsentanten vom Grad $< r$ der Elemente von $\mathbb{F}_q$.

3. Wir ersetzen im RSA-Kryptosystem $\mathbb{Z}$ durch $\mathbb{F}_p[x]$, d.h. statt $n = p \cdot q$ das Produkt zweier Primzahlen, schreiben wir $f = g \cdot h$ das Produkt zweier irreduzibler Polynome aus $\mathbb{F}_p[x]$.

   Bob wählt also 2 irreduzible Polynome g und h aus $\mathbb{F}_p[x]$, berechnet $f = g \cdot h$ und

   $$\begin{aligned}\varphi(f) &= ord\left(\left(\mathbb{F}_p[x]/(g)\right)^*\right) \cdot ord\left(\left(\mathbb{F}_p[x]/(h)\right)^*\right) \\ &= \left(p^{\deg g} - 1\right) \cdot \left(p^{\deg h} - 1\right)\end{aligned}$$

   Dann wählt Bob ein zufälliges e mit $ggT(e, \varphi(f)) = 1$ und bestimmt d mit

   $$e \cdot d \equiv 1 \bmod \varphi(f)$$

   Bobs öffentlicher Schlüssel ist dann (f, e), sein geheimer Schlüssel ist d.

   Alice kann nun eine für Bob bestimmte Nachricht $m \in \mathbb{F}_p[x]/(f)$ verschlüsseln (wobei m teilerfremd mit f sei) mittels

   $$c := m^e \bmod f$$

   Bob bekommt wieder den Klartext durch:

   $$c^d = m^{d \cdot e} = m^{\,1 + k \cdot \varphi(f)} = m \bmod f$$

   (a) Warum kann man dieses Kryptosystem leicht knacken ?

   (b) Überprüfen Sie, daß dieses Kryptosystem auch deshalb zu schwach ist, weil sich z.B. Polynome vom Grad ≈ 300 über $\mathbb{F}_{11}$ faktorisieren lassen.

4. (a) Berechnen Sie per Hand:

$$\left(\frac{3}{97}\right),\ \left(\frac{5}{389}\right),\ \left(\frac{2003}{11}\right),\ \left(\frac{5!}{7}\right)$$

   (b) Zeigen Sie

$$\left(\frac{3}{p}\right) = \left\{ \begin{array}{ll} 1 & \text{falls } p \equiv 1, 11 \bmod 12 \text{ und} \\ -1 & \text{falls } p \equiv 5, 7 \bmod 12 \end{array} \right\}$$

   (c) Zeigen Sie direkt, daß

$$\left(\frac{-3}{p}\right) = 1 \text{ falls } \quad p \equiv 1 \bmod 3$$

   (Tip: Sei g eine primitive Wurzel von $(\mathbb{Z}/p\mathbb{Z})^*$. Konstruieren Sie aus g ein Element h der Ordnung 3 und zeigen Sie, daß $(2 \cdot h + 1)^2 \equiv -3 \bmod p$).

5. Schreiben Sie ein Maple-Skript, das mit dem Legendresymbol die Anzahl der Punkte einer elliptischen Kurve über $\mathbb{F}_p$ bestimmt.

Abgabe der Aufgaben bitte als email an

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