TECHNISCHE UNIVERSITÄT BERLIN WS08/09
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. Heß
Assistent: G. Möhlmann
Abgabe: 10.2.09
www.math.tu-berlin.de/~hess/krypto-ws2008

14. Übung Kryptographie

Die Punkte, die für das Lösen der Aufgaben auf diesem Blatt vergeben werden, sind Zusatzpunkte.

1. Aufgabe

Sei p eine Primzahl und $n \in \mathbb{N}$, sowie $a, b \in \mathbb{F}_p \subseteq \mathbb{F}_{p^n}$. Sei

$$E(\mathbb{F}_{p^n}) = \{(x, y) \in \mathbb{F}_{p^n}^2 | y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

die Punktgruppe einer elliptischen Kurve. Die Abbildung

$$\phi_p : E(\mathbb{F}_{p^n}) \to E(\mathbb{F}_{p^n}),\ \mathcal{O} \mapsto \mathcal{O},\ (x, y) \mapsto (x^p, y^p)$$

wird p-Frobenius genannt. Zeigen Sie, dass $\phi_p(E(\mathbb{F}_{p^n})) \subseteq E(\mathbb{F}_{p^n})$ gilt und dass der p-Frobenius ein Gruppenhomomorphismus ist.

(5 Punkte)

2. Aufgabe

Zeigen Sie, daß DSA ohne die Verwendung von SHA-1 nicht sicher bezüglich existenzieller Fälschung unter einem key-only Angriff ist. Mit der Notation aus dem Skript kann man als Ansatz $h = gy$ versuchen.

(5 Punkte)

3. Aufgabe

Schreiben Sie ein Programm das zwei Punkte einer elliptischen Kurve über einem endlichen Körper der Charakteristik ungleich zwei oder drei addiert. Zum Testen können sie mit *EllipticCurve(q,[a,b])* in Kash die elliptische Kurve $y^2 = x^3 + ax + b$ über $\mathbb{F}_q$ erzeugen. *RandomPoint()* liefert Punkte auf der Kurve. Wenn sie mit Elementen aus $\mathbb{F}_q$ rechnen wollen, dann können Sie mit $F := GF(q)$ diesen erzeugen. Mit *Coerce*(F, n) können sie ganze Zahlen n nach F schieben.

(5 Punkte)