TECHNISCHE UNIVERSITÄT BERLIN Sommersemester 2004
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. Heß
WM: Dipl.-Math. M. Wagner
www.math.tu-berlin.de/~hess/krypto

11. Übung Kryptographie

1. Aufgabe Decision Diffie-Hellman Problem (3 Punkte)

Sei G eine zyklische Gruppe der Ordnung ℓ und g ein Erzeuger. Ein Algorithmus A für das DDH in G ist ein probabilistischer, in $\log(\ell)$ polynomieller Algorithmus, für den es ein $\alpha > 0$ und ℓ_0 mit

$$\Pr\big(A(G, \ell, g, g^a, g^b, w_s, w_{1-s}) = s \text{ für } w_0 = g^{ab}, w_1 \in_R G,\ a, b \in_R \mathbb{Z}/\ell\mathbb{Z}, s \in_R \{0,1\}\big) > 1/2 + \ell^{\alpha}$$

für alle $\ell \geq \ell_0$ gibt ($\in_R$ heißt, daß gleichverteilt zufällig ausgewählt wird).
Zeigen Sie, daß es einen Algorithmus für das DDH gibt, wenn ℓ einen in $\log(\ell)$ polynomiellen Faktor c besitzt.

2. Aufgabe Elliptische Kurven (4 Punkte)

Sei $E : Y^2 = X^3 + aX + b$ eine elliptische Kurve über $\mathbb{F}_q$ mit $q = p^r$ und $p > 3$.

1. Berechnen Sie die Koordinaten von $-P$ für $P = (x_P, y_P)$.
2. Zeigen Sie $\#E(\mathbb{F}_q) = 0 \bmod 2$ genau dann, wenn $X^3 + aX + b$ eine Nullstelle in $\mathbb{F}_q$ besitzt.

3. Aufgabe Glattheitswahrscheinlichkeit (3 Punkte)

Wir betrachten den Polynomring $\mathbb{F}_p[t]$. Die Anzahl der Primpolynome in $\mathbb{F}_p[t]$ eines Grads m ist ungefähr p^m/m.

1. Sei M eine Menge von k Primpolynomen vom Grad m und sei n teilbar durch m. Zeige, daß es mindestens $k^{n/m}/(n/m)!$ Polynome vom Grad n gibt, deren Primfaktoren sämtlich in M liegen.
2. Führen Sie eine Diskussion der erwarteten Laufzeit eines Index-Calculus Angriffs in $\mathbb{F}_q$ mit $q = p^n$ durch. Zur Vereinfachung können Sie die Annahme machen, daß n durch geeignete m teilbar ist.

4. Aufgabe Praktische Aufgabe: Diskreter Logarithmus (10 Punkte)

Implementieren Sie das Pollard rho und das Index-Calculus Verfahren zur Berechnung diskreter Logarithmen über endlichen Körpern $\mathbb{F}_q$ mit $q = p^r$, p klein und r groß. Vergleichen Sie die Laufzeiten anhand von praktischen Beispielen.

Gesamt: 20 Punkte