TECHNISCHE UNIVERSITÄT BERLIN WS06/07
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr.F. Heß
WM: Dipl.-Math. M. Wagner
www.math.tu-berlin.de/~hess/krypto-ws2006

12. Übung Kryptographie

1. Aufgabe Zero Knowledge (4 Punkte)

Sei n ein RSA-Modul, x zufällig und $y = x^2 \mod n$. Person P soll die Kenntnis von x beweisen ohne etwas über x zu verraten. Im Skript wird dazu eine Vorgehensweise angegeben. Die Bezeichnungen sind hier wie im Skript. Angenommen es gibt ein schummelndes B mit Erfolgswahrscheinlichkeit $> \frac{1}{2}$. Zeige, dass dann B Wurzeln b, r mit $b^2 = ay^e$ und $r^2 = ay^{e'}$ und $e \neq e'$ berechnen kann.

2. Aufgabe Paarungsbasierte Kryptographie (6 Punkte)

Seien G_1, G_2, G_I zyklische Gruppen von Primzahlordunung p. Eine Paarung ist eine nicht-degenerierte bilineare Abbildung

$$e : G_1 \times G_2 \longrightarrow G_I.$$

Die Gruppen G_1, G_2 und G_I sollen sicheres DLP und CDH haben. Zeige, dass wenn $G_1 = G_2$ gilt dann das DDH in G_1 mit Hilfe von e leicht zu lösen ist.

3. Aufgabe Homomorphie-Satz für Moduln (4 Punkte)

Beweisen Sie den Homomorphiesatz für unitäre R-Moduln N, M, wobei R ein kommutativer Ring mit 1 und nullteilerfrei ist.

4. Aufgabe Hermite-Normalform (6 Punkte)

Gegeben seien die Matrizen $B, A \in \mathbb{Z}^{4\times 3}$ mit

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 1 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} \text{ und } B = \begin{pmatrix} 1 & 2 & 13 \\ 0 & 10 & 1 \\ 2 & 5 & 2 \\ 1 & 22 & 13 \end{pmatrix}.$$

Zeigen Sie, daß durch die Spalten der Matrix A ein $\mathbb{Z}$-Modul gegeben und daß der Kern von A ein $\mathbb{Z}$-Modul ist. Berechnen Sie den Kern von A. Berechnen Sie den Schnitt der $\mathbb{Z}$-Moduln, die durch die Matrizen A und B erzeugt werden. Welche Information erhält man immer aus der Hermite-Normalform von A über das von A erzeugte $\mathbb{Z}$-Modul?