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`

9. Übung Kryptographie

1. Aufgabe Rabin Kryptosystem (4 Punkte)

(i) Sei $n = 713$ ein öffentlicher Rabin-Schlüssel und sei $c = 289$ ein Schlüsseltext den man durch Rabin-Verschlüsselung mit diesem Modul erhält. Bestimmen Sie alle möglichen Klartexte.

(ii) Überlegen Sie sich ein Verfahren, mit dem das Problem der Mehrdeutigkeit des entschlüsselten Klartexts beim Rabin Kryptosystem behoben wird.

2. Aufgabe Hashfunktion mittels zyklischer Gruppen (4 Punkte)

Sei G eine zyklische Gruppe der Primzahlordnung $p > 2$ und $n < p/2$. Seien $g, y \in G$ gleichverteilt zufällig gewählt. Wir definieren $M = \{0, \ldots, n\}$ und $h : M \times M \to G$ durch $(m_0, m_1) \mapsto g^{m_0} y^{m_1}$.

(i) Unter welchen (weiteren) Bedingungen an G ist h kollisionsresistent? Beweisen Sie dies!

(ii) Wie kann h dann als Hashfunktion $H : \{0, 1\}^* \to G$ verwendet werden?

3. Aufgabe ElGamal Kryptosystem und DDH (4 Punkte)

Sei G eine zyklische Gruppe. Zeigen Sie, daß sich die Sicherheit des DDH in G auf die Sicherheit des ElGamal Kryptosystems in G bezüglich IND-CPA Angriffen reduzieren läßt.

(Konkret ist also zu zeigen: Ein Algorithmus ORACLEDDH zum Lösen des DDH in G kann verwendet werden, um einen IND-CPA Angreifer gegen das ElGamal Kryptosystem in G zu implementieren. Der Angreifer soll hierbei polynomiell sein, also speziell auch nur polynomiell viele Aufrufe von ORACLEDDH tätigen.)

4. Aufgabe Quadratisches Sieb (8+12 Punkte)

Implementieren Sie das Quadratische Sieb in KASH3.

Hinweis: Die 12 Punkte sind Zusatzpunkte. Die praktische Aufgabe kann bis zum 15.01.07 abgegeben werden.