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

10. Übung Kryptographie

1. Aufgabe Diskreter Logarithmus (6 Punkte)

(i) Lösen Sie $a^x \equiv 507 \mod 1117$ für die kleinste Primitivwurzel $a \mod 1117$ mit dem Pohlig-Hellman-Algorithmus.

(ii) Berechnen Sie mit dem Pollard-ρ-Algorithmus die Lösung von $g^x \equiv 15 \mod 3167$ für die kleinste Primitivwurzel $g \mod 3167$.

(iii) Lösen Sie $3^x \equiv 693 \mod 1823$ mit Babystep-Giantstep-Algorithmus (Shanks Algorithmus)

2. Aufgabe Diffie-Hellman (4 Punkte)

Ein ElGamal-Kryptographie-Verfahren kann in beliebige zyklische Untergruppen $\langle\alpha\rangle$ mit $\alpha \in G$ irgendwelcher endlicher Gruppen G implementiert werden. Sei dazu $\beta \in \langle\alpha\rangle$, dann ist der **public key** das Tupel (α, β). Der Klartextraum ist dann $\mathcal{P} = \langle\alpha\rangle$ und für die Verschlüsselung erhalten wir $e_K(x) = (y_1, y_2) = (\alpha^k, x \cdot \beta^k)$, wobei $k \in \mathbb{N}$ zufällige gewählt wird.

(a) Angenommen ORACLEDDH ist ein Algorithmus, der das DDH löst. Zeigen Sie, daß ORACLEDDH als eine Subroutine in einem Algorithmus so verwendet werden kann, daß das Entscheidungsproblem für zwei Chiffretexte gelöst werden kann. (D.h. sind $x_1, x_2 \in \mathcal{P}$ gegeben und (y_1, y_2) ein Chiffretexte von x_1 oder x_2, so kann der Algorithmus entscheiden ob $e_K(x_1) = (y_1, y_2)$ oder $e_K(x_2) = (y_1, y_2)$ gilt).

(b) Angenommen ORACLEDISTINGUISH ist ein Algorithmus, der in der Lage ist das obige Entscheidungsproblem zu lösen und zu bestimmen, ob ein gegebener Chiffretext (y_1, y_2) ein gültiger Chiffretext zu x_1 oder x_2 ist. Zeigen Sie, daß ORACLEDISTINGUISH benutzt werden kann um das DDH zu lösen.

3. Aufgabe Praktische Aufgabe: Quadratisches Sieb (10 Punkte)

Implementieren Sie den Quadratisches Sieb Algorithmus in KASH. Auf der Krytpgraphie-Homepage befindet sich eine Datei **QuadratischesSieb**, in der sich drei Zahlen befinden. Berechnen Sie für diese Zahlen mit Hilfe Ihres Algorithmus geeignete S-Werte zu von Ihnen vorgegebenen Größen $l \in \mathbb{Z}$, die Länge Ihres Siebintervalles, und $B \in \mathbb{Z}^{>0}$ für die Faktorbasis. Finden Sie mit Hilfe dieser S-Werte geeignete Werte x und y, so daß $x^2 - y^2$ von $n \in \mathbb{N}$ geteilt wird aber n weder $(x - y)$ noch $(x + y)$ teilt. Faktorisieren Sie jeweils n. Geben Sie jeweils l und B an und die dazu berechneten Faktoren x und y.

Wichtige Befehle: FFEltToInt, PolyMove, PolyAlg, PolyToList, Factor, FF, MatKernel, MatEchelon

Gesamt: 20 Punkte