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

11. Übung Kryptographie

1. Aufgabe Authentifizierungsbaum (3 Punkte)

Entwickeln und beschreiben Sie eine konkrete Realisierung eines Authentifizierungsbaums.

2. Aufgabe Einwegfunktionen, Sicherheit des Lamport Signaturverfahrens (4 Punkte)

Sei $f : \{0,1\}^n \to \{0,1\}^n$ eine Einwegfunktion und A ein Algorithmus, welcher nach Eingabe von poly(n) Bildwerten y_i für ein y_j ein Urbild x_j mit in n signifikanter Wahrscheinlichkeit in Zeit poly(n) berechnet. Zeigen Sie, daß man unter Verwendung von A ein Urbild eines vorgegeben Bildwerts y in Zeit poly(n) mit in n signifikanter Wahrscheinlichkeit berechnen kann.

3. Aufgabe Angriffe auf DSA (5 Punkte)

1. Zeigen Sie, daß DSA ohne die Verwendung von SHA-1 nicht sicher bezüglich existenzieller Fälschung unter einem key-only Angriff ist.
2. Zeigen Sie, daß DSA ohne den Größencheck von h und u universell gefälscht werden kann, wenn nur eine Signatur gegeben ist.

4. Aufgabe Praktische Aufgabe: Diskreter Logarithmus (8 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.