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

12. Übung Kryptographie

1. Aufgabe Rabin Signaturverfahren (3 Punkte)

Entwickeln Sie im Analogieschluß zur RSA Signatur ein Signaturverfahren, welches die Rabinfunktion verwendet. Welche Probleme und Gefahren gibt es? Wie lassen diese sich beheben?

2. Aufgabe Authentifizierungsbaum (3 Punkte)

Entwickeln und beschreiben Sie eine konkrete Realisierung eines Authentifizierungsbaums.

3. 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.

4. 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.

5. Aufgabe Blinde Signatur (5 Punkte)

Entwickeln Sie ein Verfahren zur blinden Signatur durch Modifikation des Signaturverfahrens von Schnorr. Argumentieren Sie, warum Ihr Verfahren die gewünschte Funktionalität aufweist. Hinweis: Die u definierende Gleichung geeignet mit einem Zufallswert skalieren, die zu signierenden Hashwerte der Nachrichten dem Signierer vorgeben.

Gesamt: 20 Punkte