Hochschule für Technik und Wirtschaft
Studiengang Praktische Informatik
Prof. Dr.–Ing. Damian Weber

Klausur Kryptographie, WPF Praktische Informatik

24.03.2003

Name, Vorname	
Matrikelnummer	
Unterschrift	

- Tragen Sie bitte Ihren Namen und Ihre Matrikelnummer ein und unterschreiben Sie auf dem Deckblatt.
- Geben Sie bei Ihrer Abgabe alle Aufgabenblätter zurück.
- Die zur Verfügung stehende Zeit beträgt 90 Minuten.
- Die Gesamtpunktzahl beträgt 80.
- Es sind *keine* Hilfsmittel erlaubt.

Aufgabe	1	2	3	4	Σ
max. Punkte	30	10	20	20	80
Punkte					

Aufgabe 1 (Diffie–Hellmann Schlüsselaustausch) (10+15+5 P.)

Alice und Bob benutzen den Diffie–Hellmann–Schlüsselaustausch mit der Primzahl $p = 11$ und dem Erzeuger $g = 2$.

a) Zeigen Sie, daß $g = 2$ wirklich ein Erzeuger modulo 11 ist.

b) Oscar lauscht an der Leitung und erfährt, daß Alice an Bob beim Schlüsselaustausch die Nachricht 9 und Bob an Alice die Nachricht 7 gesendet hat.

Finden Sie mit Hilfe des Pohlig–Hellman–Verfahrens die geheime Zufallszahl von Alice und berechnen Sie daraus den gemeinsamen geheimen Schlüssel von Alice und Bob.

c) Unter welcher Bedingung ist die Pohlig–Hellman–Attacke gegen den Diffie–Hellmann–Schlüsselaustausch erfolgreich? Auf welche Weise kann p erzeugt werden, um diese Attacke zu verhindern?

Aufgabe 2 (RSA) **(10 P.)**

Sie haben den öffentlichen RSA–Schlüssel $n = 21, e = 5$.

Wie lautet der zugehörige private Schlüssel d?

Aufgabe 3 (ElGamal Signatur) **(10+10 P.)**

Der öffentliche ElGamal Signaturschlüssel von Alice sei $p = 11, g = 2, y = 5$ und ihr geheimer Schlüssel sei $a = 4$.

a) Welche ElGamal–Signatur berechnet Alice für die Nachricht $m = 8$, wenn sie als Zufallszahl $k = 6$ wählt?

b) Verifizieren Sie Alices Unterschrift.

Aufgabe 4 (Hashfunktionen) **(5+5+5+5 P.)**

Gegeben sei $m = 2^{160} + 1$. Die Funktion

$$h : \mathbf{Z} \longrightarrow \mathbf{Z}, \quad x \mapsto 2^{158} \cdot x \bmod m$$

liefert dann für beliebig große Zahlen einen Output von 160 Bits.

Zeigen Sie:

$$\frac{1}{2^{158}} \equiv 2^{160} - 3 \bmod m.$$

Zeigen Sie nun in den Teilen a)–c): diese Funktion erfüllt keine der Voraussetzungen für sichere Hashfunktionen.

a) preimage–resistance: finden Sie ein Urbild x von $y = 10$ im Bereich $0 \leq x < m$

b) 2nd–preimage–resistance: finden Sie ein zweites Urbild x' mit $h(x') = y$

c) collision–resistance: finden Sie zwei von x und x' verschiedene Werte w und w' mit $h(w) = h(w')$ und $w \neq w'$