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

Kryptographie

26.08.2004

Name, Vorname	
Matrikelnummer	
Unterschrift	

- Tragen Sie bitte Ihren Namen und Ihre Matrikelnummer ein und unterschreiben Sie auf dem Deckblatt.
- Halten Sie Ihren Ausweis zur Kontrolle bereit.
- Geben Sie bei Ihrer Abgabe alle Aufgabenblätter zurück.
- Geben Sie alle Lösungsblätter ab und versehen Sie jedes mit Ihrem Namen und Ihrer Matrikelnummer.
- Die zur Verfügung stehende Zeit beträgt 90 Minuten.
- Es sind *keine* Hilfsmittel erlaubt.

Aufgabe	1	2	3	4	5	Σ
max. Punkte	2	4	4	7	3	20
Punkte						

Aufgabe 1 (Teilbarkeit) **(2 P.)**

Zeigen Sie durch Rechnen modulo 3, daß für jedes $n \in \mathbf{N}$ der Ausdruck

$$n^5 - n$$

durch 3 teilbar ist.

Aufgabe 2 (Primzahlen) **(2+2 P.)**

Für $p = 15$ und $a = 4$ gilt

$$a^{p-1} = 1. \tag{1}$$

a) Zitieren Sie den kleinen Fermat'schen Satz und begründen Sie, warum man aus Gleichung (1) nicht schließen darf, daß $p = 15$ eine Primzahl ist.

b) Benutzen Sie $p = 15$ und $a = 4$ in einer Verschärfung des kleinen Fermat'schen Satzes, um zu zeigen, daß p keine Primzahl ist.

Aufgabe 3 (RSA) **(3+1 P.)**

Alice nimmt am RSA–System teil mit öffentlichem Schlüssel $n = 33$, $e = 7$.

Bestimmen Sie

a) den geheimen Schlüssel von Alice, d.h. die Primzahlen p, q und den Exponenten d,

b) den zum verschlüsselten Text $m' = 8$ gehörigen Klartext m.

Aufgabe 4 (ElGamal–Signaturen) **(3+1+3 P.)**

Bob möchte am ElGamal–System teilnehmen und wählt hierzu die Primzahl $p = 17$.

a) Bob möchte den kleinsten Erzeuger g modulo p wählen. Zeigen Sie mit Hilfe des Erzeugerkriteriums, daß Bob sich auf $g = 3$ festlegt.

b) Bob wählt als geheimen Schlüssel $a = 11$. Geben Sie Bobs öffentlichen Schlüssel an.

c) Sie erhalten per Internet die angeblich von Bob digital signierte Nachricht $m = 5$ als

$$(m, r, s) = (5, 12, 5).$$

Hat Bob diese Nachricht signiert?

Aufgabe 5 (Zertifikate) **(3 P.)**

Nennen Sie die Bestandteile eines X.509 Zertifikates.