Klausur Datensicherheit

Semester:	AI5, Bachelor	**SS 08**,	12.7.2008
Bearbeitungszeit:	60 Minuten	Hilfsmittel:	nicht prog. C

Auf jedem Blatt Name eintragen! — Punkteangaben ohne Gewähr!

Aufgabe 1 (2 Punkte)

Warum wird eine Public-Key-Infrastruktur benötigt?

Aufgabe 2 (2 Punkte)

Handgeschriebene Signaturen dürfen nicht vom signierten Dokument getrennt werden. Digitale Signaturen hingegen können zum Beispiel unabhängig vom Dokument verschickt oder gespeichert werden. Warum?

Aufgabe 3 (5 Punkte)

Sie erhalten eine mit GNUPG digital signierte E-Mail. Welche Schritte müssen Sie ausführen um die Signatur zu überprüfen?

a) Nur bei der ersten E-Mail von diesem Sender:

b) Bei jeder E-Mail von diesem Sender:

Aufgabe 4 (4 Punkte)

Zeigen Sie, dass das Vertauschen der Bits b_1 und b_2 in einem Vektor (b_1, b_2) eine lineare Abbildung ist und geben Sie diese Abbildung an.

Aufgabe 5 (6 Punkte)

Für die Schlüsselerzeugung bei RSA seien die Primzahlen $p = 13$ und $q = 7$ gegeben, sowie der öffentliche Exponent $e = 5$.

a) Verschlüsseln Sie den Klartext $M = 44$ mit RSA.

b) Zeigen Sie, dass $d = 29$ der zugehörige geheime Exponent ist.