Klausur Datensicherheit

Semester:	AI7, WI5	**SS 07**,	4.7.2007
Bearbeitungszeit:	90 Minuten	Hilfsmittel:	nicht prog. C

Auf jedem Blatt Name eintragen! — Punkteangaben ohne Gewähr!

Aufgabe 1 (6 Punkte)

a) Was ist eine Permutation?

b) Geben Sie für folgende Zyklen die Permutation an: `A-Z-Y-B-A, C-C, D-E-F-G-H-I-D, J-J, K-K, L-M-N-O-P-L, Q-R-Q, S-T-U-V-W-X-S`.

Aufgabe 2 (6 Punkte)

Was müssen Sie als Anwender beim Einrichten von SSH tun, damit Ihre SSH-Verbindungen sicher sind (d.h. dass mit einem Public Key Verfahren authentifiziert und verschlüsselt wird)?

Aufgabe 3 (6 Punkte)

a) Warum ist der RSA-Algorithmus zum Verschlüsseln von Emails in der Praxis ungeeignet?

b) Wie wird das Problem (z.B. in GPG) gelöst?

Aufgabe 4 (12 Punkte)

a) Beweisen Sie, daß 28 keine Primzahl ist. Verwenden Sie dazu nicht die Faktorisierung von 28, sondern einen Satz aus der Vorlesung.

b) Alice hat zum Verschlüsseln mit RSA bei dem Modul $n = 91$ den öffentlichen Schlüssel $e = 7$ gewählt. Knacken Sie diesen Schlüssel und geben Sie den geheimen Schlüssel an.

c) Gibt es eine multiplikative Inverse zu 272 in $\mathbb{Z}_{858}$? (Begründung!)

Aufgabe 5 (6 Punkte)

Kreuzen Sie in folgender Tabelle alle nach dem deutschen Signaturgesetz zutreffenden Felder an:

Eine Email vom unten angegebenen Typ enthält: ⇒	keine Signatur	elektronische Signatur	fortgeschrittene elektronische Signatur	qualifizierte elektronische Signatur
mit GnuPG signierte Email				
mit X.509 signierte Email				
Email mit Namensangabe				
per zertifizierter Chipkarte auf sicherem Kartenleser signierte Email				
anonyme Email				
per Chipkarte signierte Email				