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?

Die Sicherheit des Public-Key-Verfahrens hängt von der Vertrauenswürdigkeit der Public-Keys ab. Die PKI hilft bei der Prüfung, ob ein Public-Key auch wirklich zu der jeweiligen Person/Einrichtung gehört.

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?

Eine digitale Signatur enthält den Hash-Wert des unterzeichneten Dokuments. Damit ist eine Manipulation am Dokument so gut wie unmöglich. Gleichzeitig ist die Signatur auch nur für dieses Dokument gültig, da andere Dokumente andere Hash-Werte haben. Bei handgeschriebenen Signaturen kann bei einer Trennung nicht nachvollzogen worden, was diese Unterschrift signierte oder ob das Dokument noch geändert wurde.

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:

Den Public-Key des Senders besorgen. Wenn dieser nicht von einem Trust-Center signiert wurde, muss geprüft werden, ob dieser wirklich dem Sender gehört. Dies sollte auf einem sicheren Kanal erfolgen.

b) Bei jeder E-Mail von diesem Sender:

Prüfen, ob sich der Public-Key des Senders eventuell geändert hat.

ohne Gewähr :-)

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.

```
(b1, b2) -----> (b2, b1)

        | b1
        | b2
------------
A11 A12 | b2   => A11*b1 + A12*b2 = b2 => A11 = 0; A12 = 1
A21 A22 | b1   => A21*b1 + A22*b2 = b1 => A21 = 1; A22 = 0

A = |0 1|
    |1 0|

Matrix-Multiplikation ist eine lineare Abbildung
```

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.

```
n = 13*7 = 91
phi(n) = (13-1)*(7-1) = 12*6 = 72 (für b-Teil)

E(44) = 44^5 mod 91 = 18
```

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

```
Es muss gelten: e*d mod phi(n) = 1
5*29 mod 72 = 145 mod 72 = 1

Alternativ (umständlich): d über erweiterten Euklid berechnen
```