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?

Eine Abbildung, eine Vertauschung der Elemente einer endlichen Menge.

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`.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Z A C E F G H I D J K M N O P L R Q T U V W X S B Y

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)?

- Schlüsselpaar generieren

- Public-Key sicher zum Server bringen

ka was noch ...

Aufgabe 3 (6 Punkte)

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

RSA benötigt relativ viel Rechenzeit zum Ver-/Entschlüsseln.

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

Es kommt eine hybride Verschlüsselung zum Einsatz. Die eigentliche Nachricht wird mit einem symmetrischen Verfahren verschlüsselt. Der dabei verwendete Schlüssel wird mit RSA verschlüsselt.

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.

```
Fermat: n prim => a^(n-1) mod n = 1 für alle a = 1..(n-1)
a = 1: passt immer
a = 2: 2^27 mod 28 = ?
       2^27 ist sicher eine gerade Zahl. Der Divisionsrest zweier
       geraden Zahlen ist immer gerade, also ungleich 1
       => 28 ist keine Primzahl
(Zur Hilfe: Wenn man die Division durch eine wiederholte Subtraktion
ersetzt, ist klar, dass der Rest gerade sein muss)
```

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.

```
p * q = 91 => eine Zahl muss kleiner oder gleich der Wurzel von 91
   sein, die andere Zahl größer sein.
   also: 2 <= p <= Wurzel(91); Wurzel(91) <= q <= 91
   => 2 <= p <= 9  [10 muss nicht getestet werden, da es bereits im
                    Zahlenbereich von q ist]

91 / 2 = 40,5 => passt nicht, 4;6;8 streichen
91 / 3 = 30,3... => passt nicht, 9 streichen
91 / 5 = 18,2 => passt nicht
91 / 7 = 13 => Treffer
p = 7; q = 13
phi(n) = (7-1)*(13-1) = 72

ggT(72, 7):
72 = 10*7 + 2
 7 =  3*2 + 1

erweiterter Euklid:
 1 = 7 - 3*2
   = 7 - 3*(72-10*7)
   = 7 - 3*72 +30*7
   = 31*7 mod 72
=> d = 31
```

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

```
Wenn es eine multiplikative Inverse gibt, müssen 858 und 272
teilerfremd sein also ggT = 0. Man sieht schon dass beide Zahlen
den Faktor 2 enthalten. => nein
Trotzdem noch die Rechung: ggt(858, 272):
858 = 3*272 + 42  | 42 = 2*20 + 2
272 = 6*42 + 20   | 20 = 10*2          => ggT(858, 272) = 2
```

Aufgabe 5 (6 Punkte) OHNE GEWÄHR !!!

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		x		
mit X.509 signierte Email		x		
Email mit Namensangabe	x			
per zertifizierter Chipkarte auf sicherem Kartenleser signierte Email				x
anonyme Email	x			
per Chipkarte signierte Email			x	