Klausur Datensicherheit

Semester:	AI7, WI5	**SS 06**,	17.7.2006
Bearbeitungszeit:	90 Minuten	Hilfsmittel:	Keine

Punkteangaben ohne Gewähr!

Aufgabe 1 (6 Punkte)

a) Wozu dient der Friedmann-Test?

Er dient der ungefähren Bestimmung der Schlüssellänge bei einer Vigenère-Chiffre. Sollte zusammen mit Kasiski-Test angewendet werden.

b) Gegeben sei ein Chiffretext über dem Alphabet $(A, B, C, \ldots Z)$. Welche Größen müssen Sie ermitteln als Eingabewerte für den Friedmann-Test?

Es werden die Häufigkeiten der einzelnen Buchstaben des Chiffretext als Eingangsgrößen benötigt. [Koinzidenzindex des Ausgangstextes muss bekannt sein.]

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
- Schlüssel sicher zum Server bringen
... ka was noch (für 6 Punkte bisschen wenig)

Aufgabe 3 (6 Punkte)

Authentifikation mit digitalen Signaturen kann z.B. wie folgt durchgeführt werden:

Alice	unsicherer Kanal	Bob
	$\xleftarrow{r}$	wählt Zufallszahl r
signiert r		
	$\xrightarrow{E_{S_A}(r)}$	$D_{P_A}(E_{S_A}(r)) \stackrel{?}{=} r$

a) Welchen Vorteil bietet dieses Protokoll gegenüber dem Challenge-and-Response-Protokoll?

Der Server muss das Passwort nicht im Klartext speichern.

b) Welche Vorteile bietet dieses Protokoll gegenüber der Authentifikation mittels Passwort und Speicherung des Hashwerts des Passworts?

Speicherung der Hashwarte ermöglicht Wörterbuchangriffe wenn Hash-Werte an einen Angreifer kommen. Speicherung der Hash-Werte ermöglicht außerdem Replay-Angriffe (Anmeldung abhören und nachmachen).

Aufgabe 4 (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 5 (12 Punkte)

a) Beweisen Sie, daß 251 eine Primzahl ist.

```
Beweis lediglich über Faktorisierung möglich. Alle Zahlen bis
Wurzel(251) testen, also 2 bis 15 (16 ist bereits zu groß)
251 / 2 = 125,5 => passt nicht, 4;6;8;10;12;14 streichen
251 / 3 = 83,6... => passt nicht, 9;15 streichen
251 / 5 = 50,2 => passt nicht
251 / 7 = 7,86 => passt nicht
251 / 11 = 22,82 => passt nicht
251 / 13 = 19,31 => passt nicht  ==> prim, keine Faktorisierung mgl
```

b) Berechnen Sie mit Hilfe des Fermat'schen Satzes die multiplikative Inverse zu 16 in $\mathbb{Z}_{17}$.

```
Fermat: a^(-1) = a^(n-2) in Zn
16^(-1) = 16^15 = 16^8 * 16^4 * 16^2 * 16 mod 17
        = ((16^2)^2)^2 * (16^2)^2 * 16^2 * 16 mod 17
        = (256^2)^2 * 256^2 * 256 * 16 mod 17
        = (1^2)^2 * 1^2 * 1 * 16 mod 17
        = 16

da 256 mod 17 = 1
```

c) Berechnen Sie mit dem erweiterten Euklidischen Algorithmus 10^{-1} mod 113.

```
113 = 11*10 + 3
 10 = 3*3 + 1

  1 = 10 - 3*3
    = 10 - 3*(113 - 11*10)
    = 10 - 3*113 + 33*10
    = 34*10 mod 113

Prüfen:
1. Mgl: 34*10 / 113 = 340 / 113 = 3,008
   Rest: 0,0088 * 113 = 1    => passt
2. Mgl: Das erwartete Ergebnis 1 vor der Division auf die andere
   Seite bringen:
   (34*10 - 1) / 113 = 339 / 113 = 3
   Da Ganzzahl (kein Rest) passt es
```

d) Gibt es eine multiplikative Inverse zu 273 in $\mathbb{Z}_{858}$? (Begründung!)

```
Wenn 858 und 273 teilerfremd sind, gibt es eine multiplikative Inv.
ggT(858, 273):
858 = 3*273 + 39
273 = 7*39 => ggT(858, 273) = 39 => nicht teilerfremd
=> nicht möglich
```