Klausur Datensicherheit

Semester:	AI7, WI5	**SS 04**,	7.7.2004
Bearbeitungszeit:	90 Minuten	Hilfsmittel:	Keine

Punkteangaben ohne Gewähr!

Aufgabe 1 (12 Punkte)

Alice will sich den öffentlichen Schlüssel von Bob besorgen. Sie kennt Bob noch nicht persönlich und hat weder eine sichere Netzwerkverbindung zu Bob noch die Möglichkeit ihn zu besuchen oder mit ihm zu telefonieren.

a) Sie lädt Bob's öffentlichen Schlüssel von einem Keyserver herunter und benutzt diesen dann. Warum ist damit die Authentizität von Bob's Schlüssel noch nicht gesichert?

Nicht sicher, dass es Bobs Schlüssel ist. Jemand anders könnte Schlüssel hochgeladen haben, Man-in-the-Middle-Angriff, Server vertrauenswürdig?

b) Was müssen Alice und Bob und das Trustcenter tun, um die Authentizität von Bob's Schlüssel sicherzustellen?

Bob muss seinen Public-Key beim Trusctcenter authentifizieren lassen, z.B. durch PostIndent oder durch persönliches Erscheinen die Identität dem Trustcenter nachweisen. Das Trustcenter signiert Bobs Public-Key mit dem eigenen Private-Key.

Alice muss den Public-Key des Trustcenters haben (und diesem vertrauen).

Aufgabe 2 (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?

b) Welche Vorteile bietet dieses Protokoll gegenüber der Authentifikation mittels Passwort und Speicherung des Haschwerts 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 3 (5 Punkte)

Welche der folgenden Strukturen sind Körper? (ankreuzen)

☒ $\mathbb{Z}_2$ ☐ $\mathbb{Z}_8$ ☐ $\mathbb{Z}_9$ ☒ $\mathbb{Z}_{11}$ ☐ $\mathbb{Z}_{64}$ ☐ $\mathbb{Z}_{1024}$ ☐ $GF(8)$ ☐ $GF(9)$ ☐ $GF(15)$ ☐ $GF(25)$

keine Ahnung von Galois-Körpern

Aufgabe 4 (6 Punkte)

Beweisen Sie, daß 9 keine Primzahl ist. Verwenden Sie dazu nicht die Faktorisierung von 9, sondern einen Satz aus der Vorlesung.

```
Fermat: n prim => a^(n-1) mod n = 1 für a = 1..(n-1)
2^8 mod 9 = 128 mod 9 = 2 => keine Primzahl
```

Aufgabe 5 (6 Punkte)

Die S-Box Nr. 1 von DES bildet die in der Tabelle angegebenen Eingaben auf die entsprechenden Ergebnisse ab. Verwenden Sie diese Angaben und die Definition der Linearität, um zu zeigen, dass diese S-Box nichtlinear ist.

Eingabe		Ausgabe
000001	$\mapsto$	0000
000010	$\mapsto$	1110
000011	$\mapsto$	1111

```
Linearität: f(x) XOR f(y) = f(x XOR y)
f(000001) = 0000
f(000010) = 1110
f(000011) = 1111

f(000001) XOR f(000010) = 0000 XOR 1110 = 1110
f(000001 XOR 000010) = f(000011) = 1111 != 1110 => nicht linear
```