Klausur Datensicherheit

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

Punkteangaben ohne Gewähr!

Aufgabe 1 (12 Punkte)

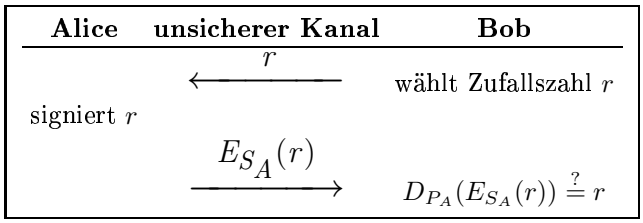
Alice will sich den öffentlichen Schlüssel von Bob besorgen. Sie kennt Bob noch nicht persönlich und hat weder eine sichere Netzwerkverbindung zu Bob noch die Möglichkeit ihn zu besuchen oder mit ihm zu telefonieren.

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?

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

Aufgabe 2 (6 Punkte)

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



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?

Aufgabe 3 (5 Punkte)

Welche der folgenden Strukturen sind Körper? (ankreuzen)

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

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.

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