Klausur Datensicherheit

Semester:	AI5, Bachelor	**SS 09**,	5.7.2009
Bearbeitungszeit:	60 Minuten	Hilfsmittel:	nicht prog. C

Auf jedem Blatt Name eintragen! — Punkteangaben ohne Gewähr!

Aufgabe 1 (5 Punkte)

a) Was ist das Kerkhoffs-Prinzip?

b) Warum ist dieses so wichtig? Nennen Sie mindestens 3 Gründe.

Aufgabe 2 (5 Punkte)

a) Wie funktioniert der CBC-Modus bei Blockchiffren?

b) Welchen Vorteil bietet er gegenüber dem ECB-Modus?

Aufgabe 3 (3 Punkte)

Wozu werden Einweg-Hashfunktionen in der modernen Kryptographie verwendet? Nennen Sie 3 Anwendungen.

Aufgabe 4 (5 Punkte)

Alice will sich auf dem Server Bob mittels Digitaler Signatur authentifizieren.

a) Beschreiben oder skizzieren Sie den Ablauf.

b) Warum ist diese Art der Authentifikation besser als das klassische Passwortverfahren mit Einweg-Hash-Funktion?

Aufgabe 5 (4 Punkte)

Was ist die zentrale Aufgabe einer Public Key Infrastruktur? (mit Begründung)

Aufgabe 6 (7 Punkte)

Gegeben seien der öffentliche Schlüssel $e = 7$ und der Modul $n = 85$ für den RSA-Algorithmus. Knacken Sie diese Chiffre, indem Sie den zugehörigen geheimen Schlüssel bestimmen.