Klausur Datensicherheit

Semester:	AI5, WI5	**Sommersemester 03**,	16.7.2003
Bearbeitungszeit:	90 Minuten	Hilfsmittel:	nicht prog. Taschenrechner

Aufgabe 1 (10 Punkte)

Gegeben sei ein Chiffretext C, der mit einer Vigenére-Chiffre verschlüsselt wurde.

a) Welche elementaren Informationen ermitteln Sie aus C beim Kasiski-Test?

b) Wie bestimmen Sie daraus die Schlüssellänge?

c) Welche elementaren Informationen ermitteln Sie aus C beim Friedmann-Test?

d) Wie bestimmen Sie daraus die Schlüsselwortlänge?

Aufgabe 2 (15 Punkte)

a) Zeigen Sie, dass das One-Time-Pad korrekt ist, d.h. dass sich nach dem Entschlüsseln wieder der Klartext ergibt. (3)

b) Für die Sicherheit des RSA-Algorithmus ist es wichtig, dass es viele Primzahlen gibt. Warum? (3)

c) Berechnen Sie die ungefähre relative Anzahl aller ganzen Zahlen, zwischen 1 und 10^9 die prim sind. (3)

d) Bestimmen Sie den geheimen RSA-Schlüssel bei dem öffentlichen Schlüssel $e = 3$ und Modul $n = 55$. (6)

Aufgabe 3 (5 Punkte)

a) Was ist eine Public Key Infrastruktur?

b) Nennen Sie den Grund für die Notwendigkeit einer Public Key Infrastruktur.

Aufgabe 4 (10 Punkte)

Berechnen Sie mit dem erweiterten Euklidischen Algorithmus $9^{-1} \bmod 113$.

Aufgabe 5 (5 Punkte)

Warum ist (heute) ein biometrisches System kein Ersatz für eine kryptographische Authentifikation?