Fachhochschule Wiesbaden
Fachbereich Design Informatik Medien
Studiengang Allgemeine Informatik
Prof. Dr. Bernhard Geib

WS 2007/08

Klausur
Security AI
LV 3151

Name:
Vorname:
Matr.-Nr.:
Unterschrift:
Note:

Sie erhalten eine geheftete Klausur. Bitte lösen Sie die Heftung **nicht**. Bitte tragen Sie zu Beginn der Bearbeitungszeit Ihren Namen, Ihren Vornamen und Ihre Matrikelnummer an den dafür vorgesehenen Stellen ein und unterschreiben Sie die Klausur. Die Klausur ist nur mit Unterschrift gültig. Die Klausur muss mit dem Verlassen des Raumes abgegeben werden.

Bearbeitungsdauer: 100 Minuten

Erlaubte Hilfsmittel: Taschenrechner

Punktevergabe:

Aufgabe	Soll-Punkte	Ist-Punkte
1	15	
2	15	
3	20	
4	10	
5	20	
6	10	
7	10	
Gesamt	100	

Zum Bestehen der Klausur müssen mindestens **50 Punkte** erreicht werden!

Aufgabe 1 (15 P.)

a) Welche Hauptbestandteile weist ein Sicherheitskonzept auf?

b) Nennen Sie mindestens drei mögliche Ziele der Netzwerksicherheit.

c) Welche Empfehlungen sollte man unbedingt beachten, um die Risiken beim Online-Kauf via Internet zu begrenzen?

Aufgabe 2 (15 P.)

a) Was versteht man unter einer Qualifizierten elektronischen Signatur?

b) Wofür werden im Internet Zertifikate benötigt?

c) Welche Aufgaben übernehmen Zertifizierungsstellen (sog. Certification Authority oder auch Trust Center)?

Aufgabe 3 (20 P.)

Wir betrachten eine (monoalphabetische) affine Tauschchiffre über dem Alphabet $A = \{a, b, ..., z\}$ mit der folgenden Chiffrierfunktion:

$$\mathbf{E}: \quad z' \equiv (z \cdot t + k) \bmod n$$

wobei

$$t = 3 \text{ und } k = 1.$$

a) Wie lautet die entsprechende Dechiffrierfunktion **D** in allgemeiner Form?

b) Berechnen Sie die Schlüsselparameter der Dechiffrierfunktion **D**.

c) Welchem Klartext-Zeichen entspricht das Chiffre-Zeichen „e“?

Aufgabe 4 (10 P.)

Berechnen Sie die Zeit (Erwartungswert) für das Knacken eines 56 Bit langen Schlüssels mit einem Brute-Force-Angriff unter der Annahme, dass Sie einen Datenblock von 64 Bit im Klartext und im Chiffretext vorliegen haben. Nehmen Sie ferner an, dass Sie Zugriff auf einen Rechner haben, der pro Sekunde 1 Megabit verschlüsseln kann.

Aufgabe 5 (20 P.)

a) Wie viele multiplikative Chiffren gibt es in $\mathbf{Z}_{26}$?

b) Wie viele verschiedene Tauschchiffren gibt es auf dem Alphabet $\mathbf{A} = \{a, b, ..., z\}$?

c) Berechnen Sie mit Hilfe eines Taschenrechners die Zahl $z = 257^{887} \bmod 31$.

d) Ermitteln Sie die Anzahl $\pi'(a, b)$ der Primzahlen im Intervall [a, b] mit $a = 10^6$ und $b = 10^9$.

Formal: $\pi'(a, b) = \#p_k$, $p_k \in \mathbf{P}$ wobei $a \leq p_k \leq b$ für $k = 1, 2, ..., \pi'(a, b)$

Aufgabe 6 (10 P.)

a) Berechnen Sie mit Hilfe des erweiterten Euklidischen Algorithmus die Lösung (x, y) der Gleichung $63 \cdot x + 36 \cdot y = 27$, sofern diese existiert. Bei der Lösung bitte vollständigen Rechengang angeben!

b) Berechnen Sie die modulare Inverse der Zahl 15 im Ring $\mathbf{Z}_{1276}$!

Formal: $15^{-1} \bmod 1276 = ?$

Aufgabe 7 (10 P.)

a) Es sei $n = p \cdot q$ mit $p, q \in \mathbf{P}$ (Menge der Primzahlen). Zeigen Sie, dass aus $x \equiv a \pmod{p}$ und $x \equiv a \pmod{q}$ folgt: $x \equiv a \pmod{n}$.

b) Es seien $a \in \mathbf{N}$ (Menge der natürlichen Zahlen) sowie $p, q \in \mathbf{P}$ (Primzahlen). Die Zahl a sei ferner kongruent 1 modulo p und kongruent 0 modulo q, d. h.

$$a \equiv 1 \pmod{5} \quad \text{und} \quad a \equiv 0 \pmod{17}$$

Wie lautet die Zahl a? (Bitte den Berechnungsweg vollständig angeben!)