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

WS 2010/2011

Klausur
Security AI

Modul 3151 (B Sc)

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: 90 Minuten

Erlaubte Hilfsmittel: Taschenrechner, Formelsammlung

Punktevergabe:

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

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

_____ Erstprüfer

_____ Zweitprüfer

Aufgabe 1 (10 P.)

Damit elektronische Geschäftsprozesse sicher und zuverlässig abgewickelt werden können, bedarf es neben einer entsprechenden Sicherheitskonzeption der Implementierung geeigneter Sicherheitsmaßnahmen. Beantworten Sie vor diesem Hintergrund die folgenden Fragen:

a) Welche Sicherheitsvorkehrungen sind erforderlich, um E-Mails zu einem seriösen E-Business-Werkzeug zu machen?

b) Nennen Sie mindestens drei verschiedene Arten von kryptographischen Angriffen auf ein Kryptosystem?

c) Wann gilt ein Kryptoalgorithmus als sicher und wann als uneingeschränkt sicher?

d) Welche Eigenschaften besitzt eine gute elektronische Unterschrift?

e) Was versteht man unter einer fortgeschrittenen elektronischen Signatur?

Aufgabe 2 (10 P.)

a) Bestimmen Sie sämtliche Teiler der Zahl 3^n.

b) Sei $n \in \mathbb{N}$ eine natürliche Zahl. Zeigen Sie:

b1) n ist ungerade $\Rightarrow$ n^2 ist ungerade

b2) n ist gerade $\Rightarrow$ n^2 ist gerade

c) Zeigen Sie, dass es keine Primzahlen $p \in \mathbb{P}$ gibt, die gemeinsamer Teiler zweier aufeinanderfolgender natürlicher Zahlen n und $n + 1$ sind.

d) Zeigen Sie oder widerlegen Sie die Behauptung, dass für alle ganzen Zahlen a, b und c gilt: $c \mid a$ und $c \mid b \Rightarrow c \mid (3a + 5b)$

e) Zeigen Sie: Sind $p_1, p_2, \ldots, p_n$ Primzahlen, die bei Division durch 4 den Rest 1 ergeben, dann hat ihr Produkt $p_1 \cdot p_2 \cdot \ldots \cdot p_n$ ebenfalls den Rest 1 bei Division durch 4.

Aufgabe 3 (10 P. – je richtige Antwort 1 P.)

Beantworten Sie folgende Fragen mit einer möglichst kurzen Antwort!

Nr.	Frage	Antwort
1	... ist die Wissenschaft, Geheimtexte aufzubrechen	
2	Das DES-Verfahren ist ein ... Krypto-verfahren	
3	Die Schlüssellänge beim RSA beträgt mindestens ... Bit.	
4	Zum Schlüsselaustausch verwendet man das ... -Verfahren	
5	Ein perfektes Chiffriersystem ist beispielsweise ...	
6	Zwei teilerfremde natürlichen Zahlen a und b erfüllen die Bedingung ...	
7	Die Zahlenklasse $\mathbf{Z}_m = \{0, 1, ..., m - 1\}$ nennt man einen ...	
8	Den Chinesischen Restsatzes verwendet man zur simultanen Lösung von ...	
9	Jede natürliche Zahl n > 1 lässt sich darstellen als Produkt von	
10	Ein Zertifikat ist die Beglaubigung eines ... Schlüssels	

Aufgabe 4 (15 P.)

Berechnen Sie die Funktionswerte folgender Funktionen:

a) ggT(249, 48) = ?

b) $\phi(525)$ = ?

c) 2^{44} mod 11 = ?

d) eEA(7, 20) = ?

Aufgabe 5 (15 P.)

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

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

wobei

$$t = 5 \text{ und } k = 7.$$

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 „ r “?

Aufgabe 6 (20 P.)

a) Beweisen Sie: Man kann jeder natürliche Zahl $n > 1$ als endliches Produkt (mit mindestens einem Faktor) ausschließlich von Primzahlen schreiben.

Hinweis: Führen Sie sowohl einen Existenzbeweis als auch einen Eindeutigkeitsbeweis!

b) Sei $n \in \mathbb{N}$ eine zusammengesetzte natürliche Zahl. Zeigen Sie, dass n dann einen Primteiler $p \in \mathbb{P}$ mit $p \leq \sqrt{n}$ besitzt.

Aufgabe 7 (20 P.)

a) Bestimmen Sie die simultane Lösung (kleinste positive ganze Zahl x) folgender linearer Kongruenzen:

$$x \equiv 3 \pmod{17}$$

$$x \equiv 10 \pmod{16}$$

$$x \equiv 0 \pmod{15}$$

(Bitte den Berechnungsweg vollständig angeben!)