Fachprüfung AI Diskrete Mathematik

Prof. Dr. Wolfgang Konen – FH Köln, Institut für Informatik

Probeklausur Februar 2009

Name:_____ Vorname: _____

Matr.-Nr.:_____ Unterschrift:_____

Klausurdauer: 60 min.

Hilfsmittel: Formelsammlung Mathematik
Skript Diskrete Mathematik
nicht-grafikfähiger Taschenrechner

Hinweise:
1. Benutzen Sie keinen Bleistift und keinen roten Stift. Heftung nicht lösen. Keine losen Blätter erlaubt.
2. Nebenrechnungen gehören in die Klausur - Schmierpapier ist nicht erlaubt.
3. Ungültige oder falsche Lösungswege durchstreichen. Der Lösungsweg muß nachvollziehbar sein.
4. Lesen Sie bitte zunächst die Aufgabenstellungen komplett durch und prüfen Sie auf Vollständigkeit und Verständlichkeit der Aufgaben!
5. Tragen Sie bitte auf diesem Deckblatt Name, Vorname, Matr.-Nr. und Unterschrift ein!

Ich wünsche Ihnen viel Erfolg!

Aufgaben		max. Punktzahl	erreichte Punktzahl
1	Secret Sharing	11	
2	Diophantische Gleichung	12	
3	Potenzen mod m	14	
4	Multiple Choice	13	
5			
6			
7			
8			
Punktzahl Gesamt:		50	

Aufgabe 1 Secret Sharing

Gegeben sei die Primzahl $p=211$ und die Teilgeheimnisse (Shares) gemäß nachfolgender Tabelle:

x_i	f_i
1	131
2	149
3	177

a) Welches ist die Geheimzahl, wenn es sich um ein (K=3)-Secret Sharing nach Shamir handelt?
b) Welches sind die Koeffizienten des zugehörigen Polynoms?
c) Wie lautet das korrekte Share für $x_i = 10$?

Aufgabe 2 Diophantische Gleichung + Algorithmus Erweiterter Euklid

Gegeben seien die beiden diophantischen Gleichungen

(1) $75x + 20y = 4$

(2) $27x - 59y = -10$

a) Welche der beiden diophantischen Gleichungen besitzt Lösungen?

b) Ermitteln Sie für diese Gleichung aus (a) eine spezielle Lösung mit dem Algorithmus Erweiterter Euklid.

c) Ermitteln Sie für diese Gleichung aus (a) alle Lösungen mit x>0, y>0.

Aufgabe 3 Potenzen mod m

Berechnen Sie mit geeigneten Rechenregeln und –tricks der Modularen Arithmetik:

a) $(121)^{38} \bmod 11$

b) $(26 \cdot 26)^{250} \bmod 5$

c) $(1235)^{39} \bmod 9$

Aufgabe 4 Multiple Choice

4.1. Kreuzen Sie alle Aussagen an, die wahr sind!

a) ☐ Alle Zahlen aus $\mathbf{Z}_9$ haben ein multiplikatives Inverses (mod 9).

b) ☐ Alle Zahlen aus $\mathbf{Z}_6$ haben ein multiplikatives Inverses (mod 6).

c) ☐ Alle Zahlen aus $\mathbf{Z}_7$ haben ein multiplikatives Inverses (mod 7).

4.2. Welche der nachfolgenden Anforderungen stellt man an eine kryptographische Hashfunktion H(s)?

a) ☐ Für jede Nachricht s ist H(s) leicht zu berechnen.

b) ☐ Gegeben sei $h_1 = H(s_1)$: Es ist schwer, ein weiteres s_2 mit $H(s_2) = h_1$ zu finden.

c) ☐ Einweg-Funktion: Zu gegebenem h ist es schwer, ein s mit H(s) = h zu finden.

d) ☐ kollisionsfrei: Es gibt keine zwei Nachrichten $s_1 \neq s_2$ mit $H(s_1) = H(s_2)$.