Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2008/2009
Übungsblatt 6

Abgabetermin: 03.12.2008 bis 14:00 Uhr

Achtung: Die schriftlichen Lösungen aller mit H gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben. Während des Semesters werden drei Übungsblätter korrigiert. Bei drei richtigen Lösungen erfolgt ein Bonus von zwei drittel Notenstufen auf die Klausurnote, bei zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer drittel Notenstufe.

Aufgabe 13: (K) Geburtstags-Paradoxon

a. Beweisen Sie, dass wie in der Vorlesung gezeigt mindestens 23 Personen in einem Raum anwesend sein müssen, so dass mit einer mindestens 50%igen Wahrscheinlichkeit wenigstens zwei von ihnen am selben Tag Geburtstag haben!

b. Wie viele Hashes aus nicht identischen Eingabewerten muss man demnach durchschnittlich berechnen, bevor es zu einer Kollision kommt?

Aufgabe 14: (H) Diffie-Hellman

a. Berechnen Sie die Werte der relevanten Größen, die beim Schlüsselaustausch zwischen Alice und Bob mit Hilfe des Diffie-Hellman Verfahrens entstehen. Wie lautet der ausgetauschte Schlüssel, wenn Alice den Schlüsselaustausch initiiert und als Wert für die Primzahl 23 sowie 5 als Wert für die Primitive Wurzel vorgibt. Gehen Sie davon aus, dass der geheime Schlüssel von Alice 6 und der von Bob 15 ist.

b. Versetzten Sie sich in die Lage von Eve, der die Kommunikation von Alice und Bob mithört. Kann Eve den ausgetauschten Schlüssel mit den ihm bekannten Werten berechnen?