King Fahd University of Petroleum and Minerals
College of Computer Sciences and Engineering
Department of Computer Engineering

COE 451 – Computer and Network Security (T142)

Homework # 05 ***(due date & time: Thursday 02/04/2015 during class period)***

Problem # 1: Suppose that h is a secure hash that generates an n-bit hash value.

a. What is the expected number of hashes that must be computed to find 25 collisions? That is, what is the expected number of hashes that must be computed to find pairs (x_i, z_i) with $h(x_i) = h(z_i)$, for $i = 0,1,2,..., 24$?
b. What is the expected number of hashes that must be computed to find m collisions?

Problem # 2: Solve problem 17 of Chapter 5 of the textbook.

Problem # 3: Solve problem 21 of Chapter 5 of the textbook.

Problem # 4: Consider a "2 out of 3" secret sharing scheme.

a. Suppose that Alice's share of the secret S is (1, 1.6), Bob's share is (3, 0.8), and Charlie's share is (5, 0). **What is the secret *S*? What is the equation of the line?**
b. Suppose that the arithmetic is taken modulo 13, that is, the equation of the line is of the form $(ax + by = c) \bmod 13$. Suppose that Alice's share of the secret S is (2, 8), Bob's share is (4, 12), and Charlie's share is (6, 3). **What is the secret *S*? What is the equation of the line, mod 13?**