CS 4920/5920 Applied Cryptography Spring 2018

Assignment 2

This assignment is due at the beginning of class on February 14. Please explain how you reached your answers.

Problem 1. Dice

There is a dice. In each *event*, you throw the dice and observe the number.

a. You are using a typical dice. What is the information entropy value for one event? What is the entropy value for four events?
b. Now suppose you modify the dice so that the side that originally showed number six becomes a five (the numbers 1, 2, 3, 4 occupy one side each, and 5 occupies two sides). What is the information entropy for one event? What is the entropy for four events?
c. You can further modify the dice by changing the number it shows on the sides. How would you maximize the entropy?
d. You can further modify the dice by changing the number it shows on the sides. How would you minimize the entropy?

Problem 2. Balls in a Bin

Suppose there are five red balls, three yellow balls, and four green balls in a bin. In each *event*, you pick one ball from the bin and observe the color of the ball. After observation, you put the ball back into the bin.

a. What is the value of the information entropy for an event?

b. What is the value of the entropy for five events?

c. Now you add two yellow balls in the bin and conduct the events. What is the value of the entropy for an event?

d. From Problem c. (with a total of fourteen balls in the bin), you can either add one ball of any color to the bin or subtract one ball of any color from the bin. What would your action be (add or subtract and which color) to maximize the entropy of the events?

Problem 3.

a. Determine gcd(24140,16762).
b. Determine gcd(4655,12075).
c. Determine gcd(4278,8602).

Problem 4.

Prove the following:

a. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$
b. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$
c. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
d. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Problem 5.

Prove the following:

a. For two consecutive integers n and n+1, gcd(n,n+1)=1
b. Given two integers a and b, prove that Euclidean algorithm, described in Section 2.2, yields the greatest common divisor gcd(a,b)