ECE: Information and Network Security
Homework 3
Spring 2008

Chapter 8: Book Problems 1, 3

1. It is easy to construct collisions: h(x) = h(x+p-1), for example. (However, it is fairly quickly computed (though not fast enough for real use), and it is preimage resistant.)

3. h can be computed quickly, so (1) is satisfied. However, $h(x\|0\|0\|\cdots) = x$, so it is not preimage resistant. Taking different numbers of 0-blocks yields collisions, so it is not strongly collision-free.

Chapter 10: Book Problems 5

5. Suppose we arrange the participants in a ring, like Bob > Ted > Carol > Alice > Bob. Each person starts with α and raises it to their private exponent, e.g. Bob calculates α^b. They each send their respective result to the person to their right. The next round, they take what they received and raise it to their private exponent and pass it to their right. If we repeat this two more times, they will all have calculated α^{abcd}.

Chapter 12: Book Problems 1, 2, 7

1. To approach this problem, one should use a (2, 4) threshold scheme. If we use a Shamir (2, 4) scheme, the polynomial is of the form:

$$s(x) = 5 + a_1x + a_2x^2 + a_3x^3(modp).$$

Let us take $p = 7$ and choose the polynomial $s(x) = 5+x+x^2+x^3(mod7)$ (there are many other possible choices for polynomials). Then the secret value is $s(0) = 5$, and we may choose the shares (1, 1), (2, 5), (3, 2), and (4, 5).

2. In this problem, the (2, 30) scheme requires solving for a line that interpolates the points (1, 13) and (3, 12). The slope can be calculated to be 50, and the intercept to be 64. The resulting line is given by $s(x) = 50x + 64(mod101)$. To fix the lost data, we evaluate s(x) at x = 2 to get s(2) = 63. Hence the secret is (2, 63).

7. Take a (10, 30) scheme and give the general 10 shares, the colonels 5 shares each, and the clerks 2 each. Then each of the desired groups, and no smaller groups, have the 10 shares needed to launch the missile.