CSEP 590E: Practical Aspects of Modern Cryptography

Homework #1 Due: 6:30pm Oct 11, 2016

1. In the remote coin flipping protocol presented in lecture, we partitioned the positive integers into 4 groups. Could we have made a similar protocol work with the same kind of sequential partition but only 3 groups? With 2 groups? Explain why or why not?

2. There are several different ways in which the "mod" functionality is defined and used. In lecture, we have used "mod" as a binary operator (like subtraction) which takes two arguments and produces a third as its result: $Z \bmod N = R$, where R is the unique remainder of Z divided by N as described by the division theorem (for all integers Z and positive integers N, there are unique integers Q and R with $0 \le R < N$ such that $Z = NQ + R$ and that this R is the value of $Z \bmod N$). Another form is as a binary relation (like equality) in which we say, $Z_1 \equiv Z_2 \pmod{N}$ is true if (and only if) $Z_1 - Z_2$ is a multiple of N (mathematically, there is an integer Q such that $Z_1 - Z_2 = NQ$). As a shorthand, we sometimes write $Z_1 \equiv_N Z_2$ in place of $Z_1 \equiv Z_2 \pmod{N}$.
   Show that
   a. if $Z_1 \bmod N = Z_2 \bmod N$, then $Z_1 \equiv_N Z_2$, and
   b. if $Z_1 \equiv_N Z_2$, then $Z_1 \bmod N = Z_2 \bmod N$.

3. We've used the "mod" function liberally in class – performing additional "mod" operations on intermediate values as it has suited us. Use the result of the previous exercise to justify this usage.
   a. Show that for all integers Z_1 and Z_2 and all positive integers N, $((Z_1 \bmod N) + Z_2) \bmod N = (Z_1 + Z_2) \bmod N$.
   b. Show that for all integers Z_1 and Z_2 and all positive integers N, $((Z_1 \bmod N) \times Z_2) \bmod N = (Z_1 \times Z_2) \bmod N$.

4. Use the extended Euclidean algorithm to find a positive integer $Z < 83$ such that $59Z \bmod 83 = 1$. (Don't just do an exhaustive search to find a

satisfying value Z.) If your computation produces a Z which is negative, you can translate it to an equivalent positive result by finding $Z \bmod 83$. Be sure to check that your answer satisfies the equation $59Z \bmod 83 = 1$. [Note that if you use slide 122 shown in class, "div" refers to the integer quotient from the division theorem and the slide includes two occurrences of q_1 which should be q_i. This will be corrected in the posted slides.

5. Suppose that we modified the Diffie-Hellman key exchange protocol to use multiplication instead of exponentiation. In the first step, Alice computes $A = Ya \bmod N$ instead of $A = Y^a \bmod N$, and Bob computes $B = Yb \bmod N$ instead of $B = Y^b \bmod N$. In the final step, Alice computes $K = Ba \bmod N$ instead of $K = B^a\ mod\ N$, and Bob computes $K = Ab \bmod N$ instead of $K = A^b \bmod N$. Does this multiplicative version of the Diffie-Hellman protocol give an effective secret key exchange? If so, why? If not, why not?