

MATH 13150: Freshman Seminar due May 2, 2012

Group Work # 12

Names: _____

Instructions: Clearly explain the answers to the following questions:

1. Suppose Alice and Bob are creating a password. Suppose they have chosen $A = 2$ and $p = 19$.
 - (a) If Alice chooses $k = 11$ and Bob chooses $l = 6$, then find $B \equiv A^k \pmod{p}$ and $C \equiv A^l \pmod{p}$.

 - (b) Compute the password for Alice, i.e., find $C^k \pmod{p}$.

 - (c) Compute the password for Bob, i.e., find $B^l \pmod{p}$.

 - (d) Do the two passwords match? If so, you've probably done the first problem correctly.

2. Suppose Eve is eavesdropping on Alice and Bob creating a password. Suppose they have chosen $A = 2$ and $p = 19$. Suppose Alice and Bob choose k and l , and Alice tells Bob that $B \equiv A^k \pmod{p}$ is $B = 9$, and Bob tells Alice that $C \equiv B^l \pmod{p}$ is $C = 11$. The purpose of this problem is for you to see the work involved for Eve in finding the password.

(a) For each number k from 1 to 18, find $2^k \pmod{19}$.

(b) Use your list in part (a) to find k and l .

(c) Find the password.

3. Suppose Alice and Bob have chosen $A = 3$ and $p = 31$ when creating a password. Alice has chosen $k = 13$ and she has received $C = 4$ from Bob.

(a) What is the password Alice creates?

(b) If Bob tells Alice that the password is 21, should she trust that it is really Bob?

4. Suppose Alice and Bob have agreed to use $p = 31$ and $A = 3$ to generate a password. Suppose Bob choose $l = 11$ and receives $B = 17$ from Alice.

(a) Compute the password.

(b) If Alice tells Bob that she is sending him the address of a cafe on State Street where they will meet at 3 pm, and tells him that the password is 22, should he trust that he is really hearing from Alice?

(c) Suppose Bob believes it is really Alice, and he tells her to use $k = 13$ and $n = 437$ for the RSA code, and Alice sends Bob the encoded number $C = 383$, what is the address of the cafe where he should meet Alice?