

MATH 13150: Freshman Seminar

Homework #12 Due *May 2, 2012*

Instructions: Clearly explain the answers to the following questions.

1. Suppose Alice and Bob are creating a password, and they have chosen $A = 7$ and $p = 23$. Suppose Alice chooses $k = 13$ and Bob chooses $l = 16$.
 - (a) What is the number $B \equiv A^k \pmod{p}$ that Alice sends to Bob?
 - (b) What is the number $C \equiv A^l \pmod{p}$ that Bob sends to Alice?
 - (c) What is the password that Alice computes?
 - (d) What is the password that Bob computes? Do the two passwords match?
2. Suppose Alice and Bob are creating a password, and they have chosen $A = 5$ and $p = 47$.
 - (a) If Alice chooses $k = 11$ and she receives $C = 12$ from Bob, then what is the password?
 - (b) If the next time she wants to talk to Bob, she asks Bob for the password and he tells her the password is 2, should she trust that she is really talking to Bob?
3. Suppose Alice and Bob are creating a password, and they have chosen $A = 2$ and $p = 59$.
 - (a) If Bob chooses $l = 31$ and he receives $B = 17$ from Alice, what is the password he creates?
 - (b) If the next time he wants to talk to Alice, he asks Alice for the password and Alice tells him the password is 49, should he trust that he is really talking to Alice?
4. Suppose Alice and Bob are creating a password, and they have chosen $p = 11$ and $A = 2$. Eve is viewing all of their communications, and although she does not know k and l , she knows that $B = 5$ and $C = 3$.
 - (a) What are k and l (hint: look at the powers of 2 mod 11, and find k so $2^k \equiv 5 \pmod{11}$ and find l so $2^l \equiv 3 \pmod{11}$)?
 - (b) Compute the password that Eve can use to pretend she is Alice or Bob.
5. Suppose Alice and Bob are creating a password, and they have chosen $p = 2179$ and $A = 47$.
 - (a) If Alice chooses $k = 865$ and Bob tells her that $C \equiv A^l \equiv 57$, then what is the password (you definitely want to use a modular arithmetic calculator for this one).

(b) (Not a problem): In this case, $l = 1235$. To find the password, Eve would have to find k or l , so she would have to compute $a^k \pmod{2179}$ for $k = 1, 2, \dots, 865$ before she could find the password. Picking a 300-digit prime would make this even more secure.

THE REMAINING PROBLEMS ARE BASED ON MATERIAL THAT WILL BE DISCUSSED MONDAY.

6. Use Fermat's theorem to show that 21 is not a prime, i.e., find a number a between 1 and 20 so that $a^{20} \not\equiv 1 \pmod{21}$.
7. Use Fermat's theorem to show that 9943 is not a prime, i.e., find a number a between 1 and 9942 so that $a^{9942} \not\equiv 1 \pmod{9943}$.
8. The last prime on the list of first 1000 primes on the course website is 7919. Find the first likely prime bigger than 7919, i.e., find a number $n > 7919$ so that $a^{n-1} \equiv 1 \pmod{n}$ for at least 6 different a with $1 < a < n$ (hint: skip numbers that are obviously divisible by small primes).
9. Find the first likely prime larger than 10,000,000 (ten million).