Homework 5
Melanie Rubalcaba
November 20, 2017

*Problem 1*
First, p and g would both need to be public Both parties would need to agree to make both keys, p and g, public.
Both of us would do our calculations on our own, with each of us choosing a value for a
I will choose a = 5
A = $g^a$ mod p
A = $5^4$ mod 9433 = 3125
I then send my value of 6171 to you and you send me the other value for 1218.
After receiving either values we perform the final calculations: Your Calculation: A = $3125^a$ mod 9433 My Calculation : A = $1218^5$ mod 9433 We both then recieve the result 1051.
*Problem 2*
Trudy and Eve would only be able to know the values of p, g, and both A values.
They would be unable to recover our key unless they somehow figured out both of our a values.