Group 2: Kyle, Jesus, Ying, Mason, Adam, Gage, Connor

Homework 3

2.6:

P = 1373 g = 2

A = 974 a = ?

B= ? b= 871

B = $g^b(mod\ 1373)\ =\ 2^{871}$ (mod 1373) = <u>805</u>

$g^{ab} = A^b\ (mod\ p) =\ 971^{871}\ (mod\ 1373)$ =<u>397</u>

$g^a \equiv A => 2^a(mod\ 1373) = 974$ => a = <u>587</u>

<u>Check:</u> $B^a\ =\ g^{ab} mod\ p\ =>\ 805^{587} mod\ 1373 = 397 = g^{ab}$

2.8:

P = 1373 g = 2

a.) a = 947 p = 1373

$A =\ g^a mod\ p =\ 2^{947} mod\ 1373 = 177$

b.) b = 716 m = 583 k = 877

c1 = $g^k mod\ p =\ 2^{877} mod\ 1373 = 719$

c2 = $\left(m\ \left(A^k mod\ p\right)\right) mod\ p) = \left(583(177^{877}\ mod\ 1373)\right) mod\ 1373) = 228536\ mod\ 1373 = 618$

c.) a = 299

x= $\ c1^a mod\ p =\ 719^{299}\ mod\ 1373 = 645$

m = $[c2\ (x^{-1} mod\ 1373) mod\ 1373] = 618(645^{-1}\ mod\ 1373) mod\ 1373) = 618(794) mod\ 1373 = 332$

d.) $B =\ g^b mod\ p =\ 2^{219}\ mod\ 1373 = 893$

X = $c1^b mod\ p =\ 719^{219} mod 1373 = 431$

m = $[c2(x^{-1}\ mod\ p) mod\ p] = [618(431^{-1}\ mod\ 1373) mod\ 1373] = 365$

2.17

a) x = 37

b) x = 59

Group 2: Kyle, Jesus, Ying, Mason, Adam, Gage, Connor

c) x = 319

Next, take the prime 18446744073709551629 where g = 18446744073709551628, and h = 18446744073709551628

Then x = 1