Duy Nhan Cao

2.8 $p = 1373$ $g = 2$

a. $a = 947$

$g^a \equiv 177 \pmod{1373}$

b. $b = 716$ $m = 583$ $k = 877$ $c_1 = g^k$ $c_2 = mA^k$

$(c_1, c_2) = (719, 623)$

c. $a = 299$ $A = 34$ $c_1 = g^k$, $c_2 = mA^k$

$(c_1, c_2) = (661, 1325)$

$x = c_1^a \rightarrow x = 392$

$x^{-1} = x^{p-1-1} = x^{p-2} \rightarrow x^{-1} = 693$

$x^{-1} c_2 = m \rightarrow m = 168$

$\rightarrow$

d. $2^b = 893 \pmod{1373}$ $(c_1, c_2) = (693, 793)$

$\rightarrow b = 219$

$x = c_1^b \rightarrow x = 431$

$x^{-1} = x^{p-2} \rightarrow x^{-1} = 532$

$x^{-1} c_2 = m \rightarrow m = 365$