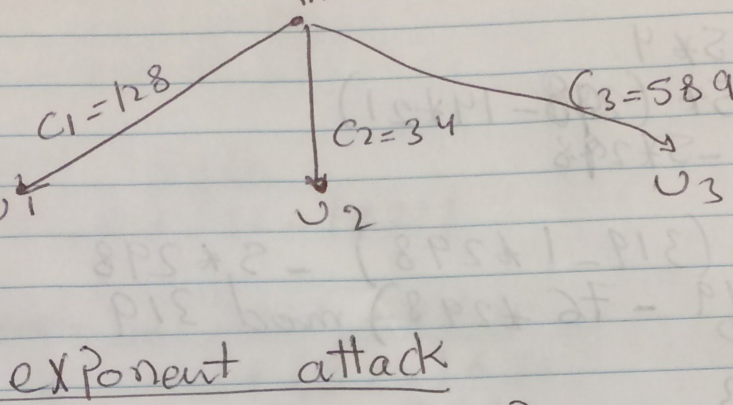
prob3

(n,e)
U1: (319,3)
U2: (697,3)
U3 = (1081,3)



low exponent attack

$C_1 = m^{e_1} \bmod n_1 \quad = m^3 \bmod 319$
$C_2 = m^{e_2} \bmod n_2 \quad = m^3 \bmod 697$
$C_3 = m^{e_3} \bmod n_3 \quad = m^3 \bmod 1081$

$X = 128 \bmod 319$
$X = 34 \bmod 697$
$X = 589 \bmod 1081$
} CRT to determine X

low exponent
$X = m^{\boxed{3}} \bmod 319*697*1081$

So $m = (X^{1/3})$

$X = [128*(\overset{753457}{697*1081})*753457^{-1} \bmod 319$

~~$+34*(\overset{222343}{319*697})*222343^{-1} \bmod 69$~~

$+34*(\overset{344839}{319*1081})*344839^{-1} \bmod 697$

$+589*(\overset{222343}{319*697})*222343^{-1} \bmod 1081\}$

$\bmod 319*697*1081$

$753457^{-1} \bmod 319 \; ? \equiv 298^{-1} \bmod 319$

$319 = 1*298 + 21$

$298 = 14*21 + 4$

$21 = 5*4 + 1$

$1 = 21 - 5*4$

$= 21 - 5*(298 - 14*21)$

$= 71*21 - 5*298$

$= 71*(319 - 1*298) - 5*298$

$= (71*\underset{0}{\cancel{319}} - 76*298) \bmod 319$

$298^{-1} = 243$

$344839^{-1} \bmod 697 \equiv 521^{-1} \bmod 697$

$697 = 1*521 + 176$

$521 = 2*176 + 169$

$176 = 1*169 + 7$

$169 = 24*7 + 1$

$1 = 169 - 24*7$

$= 169 - 24*(176 - 1*169)$

$= 25*169 - 24*176$

$= 25*(521 - 2*176) - 24*176$

$= 25*521 - 74*176$

$= 25*521 - 74*(697 - 1*521)$

$= 99*521 - 74*\underset{0}{\cancel{697}}$

$521^{-1} = 99$

$222343^{-1} \bmod 1081 = 738^{-1} \bmod 1081$

$1081 = 1*738 + 343$ ✓
$738 = 2*343 + 52$ ✓
$343 = 6*52 + 31$ ✓
$52 = 1*31 + 21$ ✓
$31 = 1*21 + 10$ ✓
$21 = 2*10 + 1$

$m = x^{1/3}$
$= 4913^{1/3}$
$= 17$

$1 = 21 - 2*10$
$= 21 - 2*(31 - 1*21)$

~~21~~ $= 3*21 - 2*31$
$= 3*(52 - 1*31) - 2*31$
$= 3*52 - 5*31$
$= 3*52 - 5*(343 - 6*52)$
$= 33*52 - 5*343$
$= 33*(738 - 2*343) - 5*343$

$= -71*343 + 33*738$

$= -71*(1081 - 1*738) + 33*738$

$= -71*1081 + 104*738$

$738^{-1} = 104$

$$x = \left[\begin{array}{l} 128*753457*243 \\ +34*344839*99 \\ +589*222343*104 \end{array}\right] \bmod 24035278$$

$= [121306577 + 199316942 + 160086960]$
$= 480710479 = 4913$