CS 427, Assignment 7

Cody Malick
malickc@oregonstate.edu

March 10, 2017

1

To get the value of m, we ultimately have to derive the value of d, our decryption exponent. To do so, we start by calculating the RSA Modulus:

$N \ = \ p * q$
$N \ = \ 9117974865455905306854905819697051438026532916687180888076306938627349875532657604237614264588159197059815174375567981463992373512122956300201579359580521523857771668102782515298344394344155055735457158213468503760021845661341787018714549993329931085779672821202518040360247980809810895818474245240280337281$

Now we need the value of $\phi(N)$:

$\phi(N) \ = \ (p-1)*(q-1)$
$\phi(N) \ = \ 9117974865455905306854905819697051438026532916687180888076306938627349875532657604237614264588159197059815174375567981463992373512122956300201579359580507754618946841515762774878258397633971509057865891091564337762218052096099462269458759233215134953898843496802257959435027441490498960112361399485603646464$

With those two numbers, we can calculate the value of d:

$d \ = \ \frac{1}{e \ mod \ \phi(N)}$
$d \ = \ 8760874022161287605542050500387767439148209173213792602642509016748994136282031327309248170674784815973921629687229809866185883687888375766251125859858033560573818375137860838525323995637862964316696208672834663959520217157609927193631392683611409041866251714943161694705196079552228765852086148853008203391$

Now that we know d, simply raise our ciphertext to the power of d:

$m \ = \ (c \ mod \ N)^d$
$m \ = \ 1223334444555556666667777777888888889999999990000000000$

And our message is “1223334444555556666667777777888888889999999990000000000”. I confirmed this by re-encrypting it with the encryption exponent e.

2

Given $\phi(N)$ and n, we can quickly find the two factors using algebra, and the quadratic equation:

$$\phi(N) = (p-1)(q-1)$$
$$N = p*q$$

$$\phi(n) = (p-1)*(q-1)$$
$$\frac{\phi(N)}{p-1} = (q-1)$$
$$\frac{\phi(N)}{p-1}+1 = q$$

And conversely:

$$\frac{\phi(n)}{q-1}+1 = p$$

We also have the other formula:

$$p = \frac{N}{q}$$
$$q = \frac{N}{p}$$

Plugging these in to create two quadratic equations:

$$0 = q^2+(Nq+q-\phi(N)q)+N$$
$$0 = p^2+(Np+p-\phi(N)p)+N$$

Plug these into the quadratic formula:

$$q = \frac{(1+N-\phi(N))+\sqrt{(1+N-\phi(N))^2-4*N}}{2}$$
$$p = \frac{(1+N-\phi(N))-\sqrt{(1+N-\phi(N))^2-4*N}}{2}$$

Using these formula, we can calculate the requested values:

p = 13071703506582537746030691218059776645988993761791975581514478
3550384410764373225534882490634747346714029248654758565923709885799257583872347
06493900130209

q = 69753531824404927370972886793693353755768382947514632265151944
8755124165887426702302511051321397209426399534784224332849550739386177318878139
260776560609

$p*q = N$

3

If x and y are known, and we know that $x^2 \equiv_N y^2$, then:

$$x^2 = y^2 \ mod \ N$$

Because of this relationship, we know also that:

$$x^2-y^2 = 0 \ mod \ N$$
$$(x-y)(x+y) = 0 \ mod \ N$$

Because we know that the left side of the equation is equal to 0 mod n, the left side is then equal to some multiple of n. With that knowledge, we know that $(x-y)$ and $(x+y)$ contain factors of N. We can then solve for the greatest common divisor of $((x+y),N)$ and $((x-y),N)$ to quickly find the factors.