CS 427, Assignment 7

Cody Malick
malickc@oregonstate.edu

March 9, 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 $\phi(N)$:

$\phi(N) \ = \ (p-1)*(q-1)$
$\phi(N) \ = \ 91179748654559053068549058196970514380265329166871808880763069386273498755326576042376142645881591970598151743755679814639923735121229563002015793595805077546189468415157627748782583976339715090578658910915643377622180520960994622694587592332151349538988434968022579594350274414904989601123613994856036464 64$

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:

$m \ = \ (c \ mod \ N)^d$
$m \ = \ 122333444455555666666777777788888888999999999000000000$

And our message is "122333444455555666666777777788888888999999999000000000". 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:
$\phi(N) \ = \ (p-1)(q-1)$
$N \ = \ p * q$

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

And conversely:

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

We also have the other formula:

$$\begin{aligned}p &= \frac{N}{q}\\ q &= \frac{N}{p}\end{aligned}$$

Plugging these in to create two quadratic equations:

$$\begin{aligned}0 &= q^2+(Nq+q-\phi(N)q)+N\\ 0 &= p^2+(Np+p-\phi(N)p)+N\end{aligned}$$

Plug these into the quadratic formula:

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

Using these formula, we can calculate the requested values:

p = 13071703506582537746030691218059776645988993761791975581514478
35503844107643732255348824906347473467140292486547585659237098857992575838723470
06493900130209

q = 69753531824404927370972886793693353755768382947514632265151944
87551241658874267023025110513213972094263995347842243328495507393861773188781390
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 $N \mid x^2 - y^2$. Then, by definition, we know that $x^2 - y^2$ is a factor of N. Then, knowing one of the factors, the other can be easily found.