

MA 341
PRELIMINARY PROJECT TO RSA ENCRYPTION
DUE: Wednesday, April 1

- 1) Compute $\phi(m)$ for your value of $m = p \cdot q$ BOTH of the following ways:
 - a) $\phi(pq) = (p - 1)(q - 1)$
 - b) Using the command Eulerphi[m].
Make sure the two values agree!
- 2) Choose a value of $e, 1 < e < \phi(m)$ that satisfies $(e, \phi(m)) = 1$.
- 3) For the value of e you chose in 2), find the solution to

$$e \cdot x \equiv 1 \pmod{\phi(m)}$$

EITHER of the following ways:

- a) By finding x, y that satisfy

$$ex + \phi(m)y = 1$$

and noting that this implies $ex \equiv 1 \pmod{m}$.

- b) By noting that x is equal to the inverse of $e \pmod{\phi(m)}$ and that by Euler's Theorem:

$$e^{\phi(\phi(m))} \equiv 1 \pmod{\phi(m)}$$

So the inverse of $e \pmod{\phi(m)}$ is $e^{\phi(\phi(m))-1}$.

(NOTE THE DOUBLE PHI!!)

- c) You want $d, 0 < d < \phi(m)$ that satisfies $ed \equiv 1 \pmod{\phi(m)}$, so you can't take x in 3 a) if $x < 0$. In order to get a solution > 0 you need to add $\phi(m)$ to your x value if $x < 0$. If you computed with 3b) then the value you obtain will be between 0 and $\phi(m)$ so will be your d value.

You should either hand in or email me:

- 1) Your value of $\phi(m)$.
- 2) Your chosen value of e . Be sure to check $(e, \phi(m)) = 1$.
- 3) Your value of $d, 0 < d < \phi(m)$ that satisfies $ed \equiv 1 \pmod{\phi(m)}$. Be sure to check that it satisfies this congruence.