Math 4330, Homework 7, 3/10/2014 : Due 3/24/2014 [1]

1. (10 points) Write a function `powmod(b,e,N)` which uses the method of repeated squarings to compute $b^e \bmod N$. A test case for this is `powmod(1234, 5678, 1984)` which should return `1152`. You may use Fermat's Little Theorem to generate plenty of other test cases, if you like.

2. (20 points) Alice is using the RSA system to receive encrypted messages and her (very weak) public key is

$$(N, e) = (109203882234822036736927, 11).$$

Bob has sent her the two-part message

$$\begin{aligned} y_1 &= m_1^e \bmod N = 45792000429743543575053, \\ y_2 &= m_2^e \bmod N = 91711179491640331429463. \end{aligned}$$

Write a program which

- factors N (re-use your Pollard-rho code for this), then
- finds an integer d such that $ed \equiv 1 \pmod{(\mathrm{p}-1)(\mathrm{q}-1)}$ (re-use your Algorithm X code for this), and finally
- recovers the numerical messages via $x_1 = y_1^d \bmod N$ and $x_2 = y_2^d \bmod N$ (use your `powmod` function for this).

These numerical messages actually correspond to a plaintext message - see if you can figure out what the text is.

3. (10 points) Estimate how long your program would have taken to recover Bob's message if p and q each had about 150 digits. Be sure to explain your methodology for the estimation.