HW4 Due 5:00pm Wednesday, May 7 on WyoCourses

This assignment consists of a single computational problem, personalized for each individual student. You will need to use Mathematica, or other symbolic computational software with comparable features. In preparation, you should review the class demonstration of RSA encryption (April 21-23).

You have intercepted a message which Bob has sent to Alice over an open channel, which he has first encrypted using Alice's public key (n, e). (Bob did *not* implement the authentication step described in class on April 23.) I have sent you Alice's public key (n, e), as well as the encrypted message, by email on April 23. Unfortunately, you do not know Alice's private key! But fortunately for you, Alice was careless in her choice of primes p and q, which were not quite large enough to ensure the security of messages sent to her. You should be able to factor n (this will take les than two minutes in Mathematica) and from this factorization, you can recover Alice's secret decryption key and figure out the message Bob sent to Alice, which is a phrase using the same scheme (A=01, B=02, ..., space=27) used in our class demonstration. Check that you are able to parse Bob's message and obtain a meaningful phrase. (You should Google the decrypted message in order to verify that this is a recognized phrase.) As proof that you have broken the encryption, you should submit to me the correct phrase by the designated due date for the assignment. (The default method is to submit this on WyoCourses; however, I will accept submissions by email.)