Secret Messages
Due March 15 (Midnight)

In this lab, we will be using the ElGamal Protocol to exchange secret messages. We will all be using the same prime p and primitive root g:

p =
808241878912418587664668869752380201227471917587049402831353579654087934716257177583988001816750842723486468130003910337833297294744103045277794137039348379685305766000049233920274403424909809118398706373176342402680527597912453031947055263965574521088574747656702199527971035049821214553730158203939

g = 2

I will email each of you a different number A which is g ** a (mod p), where a is secret to me. (Thus, I will choose a different secret a for each of you.) You will similarly send me a number B which is g ** b (mod p), where b is secret to you. You will choose a plaintext of approximately 1000 characters, encode it using your A and send me the encoded message as a simple list of integers. You will have to chop up your message into approximately 124-character blocks because all the numbers must be less than p. I will similarly encode a plaintext using B and send you an email of a list of integers. You will decode my message and send me the plaintext, and I will decode your message and read your plaintext.