CSCI 630, HW 05 - RSA Assignment

1. I have generated an RSA public key and the corresponding private key and then used the private key to encrypt a simple five-letter message. The encryption consists of five integers, one for each letter. Your task is to use the public key to decrypt the message. The alphabet used for the message is shown in Table 2. For this part you are to turn in just the single five-letter decrypted message.

   There are four instances of this problem shown below, *you are to do only one*. Here is how to determine which problem you should do:

   - Start with your seven-digit SAU student ID number, call it ID.
   - Calculate $ID \mod 60913$, call this ID-Mod.
   - Determine which problem to do using the follow table

ID-Mod is less than 10,000	**Do Problem (a)**
ID-Mod is from 10,001 to 20,000	**Do Problem (b)**
ID-Mod is from 20,001 to 40,000	**Do Problem (c)**
ID-Mod is greater than 40,000	**Do Problem (d)**

   Problem (a) The public key is $(877, 1961)$ and the encrypted message is `[1410, 1171, 261, 789, 1752]`.

   Problem (b) The public key is $(227, 493)$ and the encrypted message is `[8, 24, 1, 188, 131]`.

   Problem (c) The public key is $(2141, 4757)$ and the encrypted message is `[1778, 1, 3132, 3937, 3575]`.

   Problem (d) The public key is $(479, 1079)$ and the encrypted message is `[696, 727, 276, 679, 710]`.

2. Generate your own RSA public key and corresponding private key. These should not be the same keys used in the class example. Use your private key to encrypt the ***same message*** that I sent you. Provide me with your public key and the encrypted message. Again, the encrypted message should consists of five integers, one for each letter. I will use your public key to decrypt the message. I should get back the original message I sent to you.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Table 1: Alphabet with corresponding numeric values.

Note:

1. Here is a link to the Web page for calculating mod on large numbers:
   http://users.bestweb.net/ quenell/s2003/ma139/js/powermod.html