Math 350 – Homework 6

This homework takes you through the steps of working with the RSA cryptosystem in SAGE. I would encourage you to try it, even if you have not programmed before! I am more than happy to help with programming issues.

Finally, the website

http://www.public.iastate.edu/~roettger/350/hw/SAGERsa.html

has a complete explanation / a worked example of all SAGE commands you need for the RSA public-key cryptosystem. Apologies for the crummy website - this is copied directly from the SAGE docs, so a couple things don’t look right. Also, it is very chatty. Skip ahead by looking for ‘public key’, that is where you need to start reading.

Problem 8 - my own #1

a) Convert your own name (LASTFIRST, no blank space, all uppercase, truncated after 8 letters) into a list of ASCII codes. Concatenate the list to make a large integer \( m \). This is best done like this (slightly different from the instructions on the webpage):

\[
\text{cleartext} = 'ROETTGER' \\
\text{mlist} = \text{map}(\text{ord}, \text{cleartext}) \\
\text{mlist.reverse()} \\
\text{m} = \text{ZZ}(\text{mlist},100); \text{m}
\]

b) Encrypt \( m \) using the primes \( p = 127978673 \) and \( q = 174780863 \). Find an exponent \( e \) using \text{ZZ.random_element}(\text{phi}) \) as described in the webpage above. You have to compute \( \phi(n) = (p-1)(q-1) \) first. Make sure \( e < \phi(n) \) by executing

\[
e = e \mod \phi
\]

(this is simpler than the command \text{Integer}(\text{mod}(...,\phi)) \) which the website suggests). Encrypt the message \( m \) from part a) using \( n = pq \) and \( e \). Call the result \( c \).

c) Compute the decrypting exponent \( d \) using \text{xgcd} command for the extended Euclidean algorithm. Again, make sure that \( d < \phi(n) \). Remember that SAGE starts list indices at 0, so to pick the SECOND entry of the list \text{bezout}, you need \text{bezout}[1]. Verify that

\[
\text{mod}(de, \phi) == 1
\]

Finally, compute your digital signature

\[
\text{s} = m^d \mod n
\]

d) The message

\[
c = 12267644628975679
\]

has been encrypted using the same \( n = pq \) as above, and \( e = 3117633898051765 \). Decode this message!

Please send me an email with the subject **Math 350 hw 6**, starting with the lines

\[
m = ...
\]
\[
e = ...
\]
\[
c = ...
\]
\[
s = ...
\]
Then paste all the SAGE code lines you have used (in order) into the email – no other output please, and no printouts.