Math 350 – Homework 7

This homework takes you through the steps of working with the ElGamal cryptosystem in SAGE.

For useful commands, you can again refer to the website

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

although we are doing a different cryptosystem now, of course.

Problem 9 - my own

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)

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

b) Use the prime \( p = 127978673 \). Find a primitive root \( r \) using \( r = \text{primitive}_\text{root}(p) \). The \( r \) you get in this way is too small! Replace it by another primitive root, \( r = r^{1001} \mod p \). What condition must be true so that the new value of \( r \) is again a primitive root? Check the condition in SAGE.

c) Pick a random integer \( a \) between 1 and \( p - 1 \) just like last time, using

\[
\text{ZZ.random_element}(p-1).
\]

Let \( b = r^a \mod p \) (remember to use the power_mod function again!). You publish \( p, r, b \) and keep \( a \) secret.

d) Encrypt \( m \) from part a) using this cryptosystem. This means you pick a random number \( k < p - 2 \) and compute

\[
\gamma = r^k \mod p, \quad \delta = m \cdot b^k \mod p
\]

Your encrypted message to send to me is (\( \gamma, \delta \)).

e) The message

\[
(\gamma, \delta) = (123760417, 53877556)
\]

has been encrypted using the same \( p \) as above, and \( a = 78843192 \). Decode this message!

Please send me an email with the subject Math 350 hw 7, starting with the lines b = ... (we assume that I, not you, had picked that \( b \) and given it to you - you are playing first the role as the owner of the secret key and second the role of somebody else who only knows the public key).

\[
\gamma = ... \\
\delta = ...
\]

Then paste all the SAGE code lines you have used (in order) into the email – no other output please, and no printouts.