Project 9

Topic

- El Gamal

Objective

- To develop a deeper understanding of
- public key cryptosystems, in general
- To develop a deeper understand of public key cryptosystems based on the discrete log problem, in particular

Constraints and Other Details

- Work must run using Sage under Linux
- Due 4/11
- 15 points

Problem Specification

Do for El Gamal what you did for RSA in Project 7. Write a functioning El Gamal cipher. The cipher will be a Sage program with these functions, callable from the Sage prompt, and other functions as described below:

Pre: *size* is an exponent, as in *2^size*.
Post: program returns El Gamal parameters, large prime, p and primitive root, a mod p as defined in class and in McAndrew
param_gen(*size*)

Pre: *p* and a are returned by param_gen
Post: returns private key, *A*, and public key, *B* as defined in class and in McAndrew
key_gen(*p,a*)

Pre: *a* and *p* are returned from param_gen, *B* from key_gen. *plaintext* is a text string. Its numerical equivalent (see "Ancillary Functions," below) must be less than *p*.
Post: returns the encryption of plaintext C_1 and C_2, as defined in class and in McAndrew.
encrypt(*plaintext, a, p, B*)

Pre: C_1 *and* C_2 form the ciphertext returned from encrypt, *p* is returned by gen_param, *A* is the private key returned by key_gen, all as defined in class and in McAndrew.
Post: returns the text string decryption of the ciphertext, using the El Gamal algorithm
decrypt(C_1, C_2, p, A)

Ancillary Functions

The project requires several ancillary functions:

- El Gamal works with integers. Include the functions found in txt_num_conv.sage in my GitHub repository: .../pauldepalma/CPSC353/8-MiscFunctions.
- functions in txt_num_conf.sage convert a text string to an integer and an integer to a text string.

Submission

- Submit Project9.sage over GitHub Classroom
- Accept Link: https://classroom.github.com/a/JN2jM5CP
- 15 points