Project 10

Topic

- Diffie-Hellman

Objective

- To develop a deeper understanding public key cryptosystems, in general
- To develop a deeper understand of public key cryptosystems based on the discrete log problem
- To experiment with one of the earliest of the public key systems

Constraints and Other Details

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

Problem

Do for Diffie-Hellman what you did for El Gamal

Pre: *size* is an exponent, as in *2^size*.
Post: program returns a large prime, *p* and a primitive root, *g mod p*
param_gen(size)

Pre: *p*, g are returned by param_gen
Post: Returns computed *A* and and variable *a*, as defined in class and in McAndrew
Alice(*p,g*)

Pre: *p, g* are returned by param_gen
Post: Returns computed *B* and variable *b* as defined in class and in McAndrew
Bob(p,g)

Pre: *p* is returned by param_gen, *a* by Alice, and *B* by Bob
Post: Returns k_{alice} as defined in class and in McAndrew
Alice_Key(p,a,B)

Pre: *p* is returned by param_gen, *b* by Bob, and *A* by Alice
Post: Returns k_{Bob} as defined in class and in McAndrew
Bob_Key(*p,b,A*)

Execution Sequence

- param_gen
- Alice
- Bob
- Alice_Key
- Bob_Key

k_{alice} should be identical to k_{bob}

Submission

- Submit Project10.sage over GitHub Classroom
- Accept Link: https://classroom.github.com/a/ergVvXRb