Patrick Austin

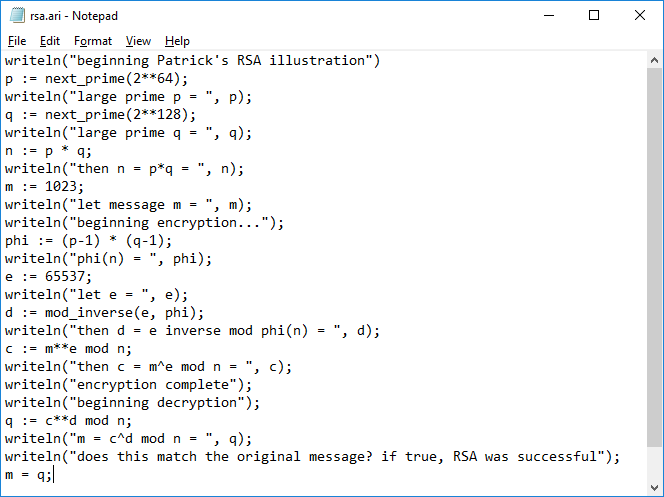
CS 450 Lab 1

9/13/2017

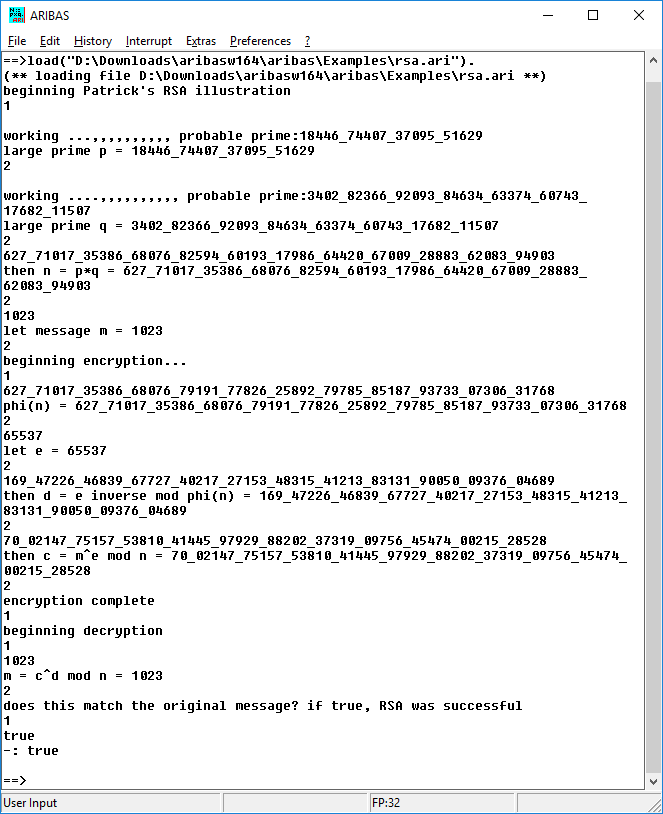
Part 1: RSA

I created a short program in ARIBAS that illustrates the execution of RSA encryption and decryption for two large primes, the first exceeding 264 and the second exceeding 2128. This verification would be exceedingly difficult to do by hand, and is far closer numerically to the real-world use case of RSA than in-class examples.

Here is a screenshot of the program’s code:



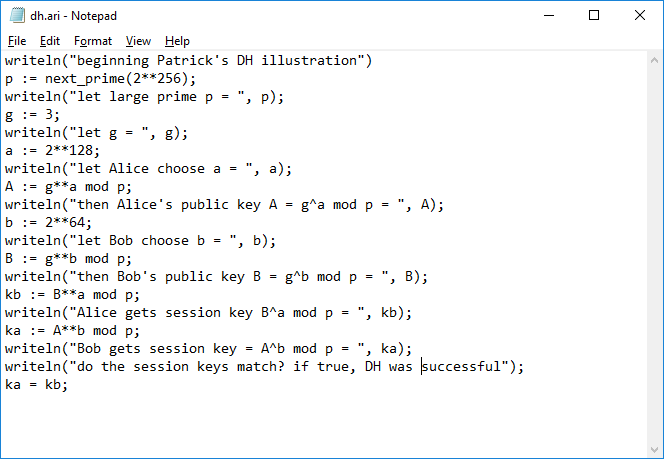
Here is a screenshot of the program executing in ARIBAS. As expected, the output of the decryption operation is the original message. Thus RSA is successfully illustrated.



Part 2: Diffie-Hellman

I also created a short program in ARIBAS that illustrates the execution of the Diffie-Hellman algorithm for a large prime p exceeding 2256. This verification would be exceedingly difficult to do by hand, and is far closer numerically to the real-world use case of DH than in-class examples.

Here is a screenshot of the program’s code:



Here is a screenshot of the program executing in ARIBAS. As expected, the users get the same session key value by conducting the DH algorithm. Thus DH is successfully illustrated.

