

CS 223 Data Structure and Algorithms

Extra Credit Assignment on the Implementation of RSA (4 points)

Question 1

This assignment is on the implementation of RSA public cryptosystem on the internet. You need to implement both the message-sending and digital signature verification part as well as a GUI so that people can use/verify. You can select n, p, q by yourself, they should be decently large (say, with at least 10 decimal digits — this is supported in JAVA).

All messages and digital signatures are decimal integers (again, within some limit, say 10 decimal digits), have a button on the interface so that people can click to check the ciphertext and also have a button so that the original message/digital signature can be shown. The final score of this assignment is based on the correctness as well as the interface of your program.

Due date: At the end of the lab on May 1, no late assignment will be accepted. I will check/grade your program in EPS 254 during the lab on May 1, so be sure to run your program on some machines in EPS 254 before then. As this is an extra credit assignment, no additional help will be provided except possibly clarifying the question. Of course, you don't have to do it if you think that you don't need the extra points.