Assignment 3 (10 marks)

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).

(1). This is the part you must do: 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.

(2). This is the part you should do (as I might give you bonus points, depending on how many people finish this part): All messages and digital signatures can also be single words like “Attack” or “George”, etc. The remaining parts are the same as in (1).

Date Due: before the end of the class on Monday, December 3, 2007 (i.e., before 5:00pm, Dec 3, 2007). You can email me the http address by email (and a grade will be emailed to you a little bit later), or come to see me during my office hours so that we can check/grade your program together in EPS 254 (be sure to run your program on some machines in EPS 254). Any late assignment will lose 2 marks for each late day.