2004.04.27

qpeN™ Test Plan

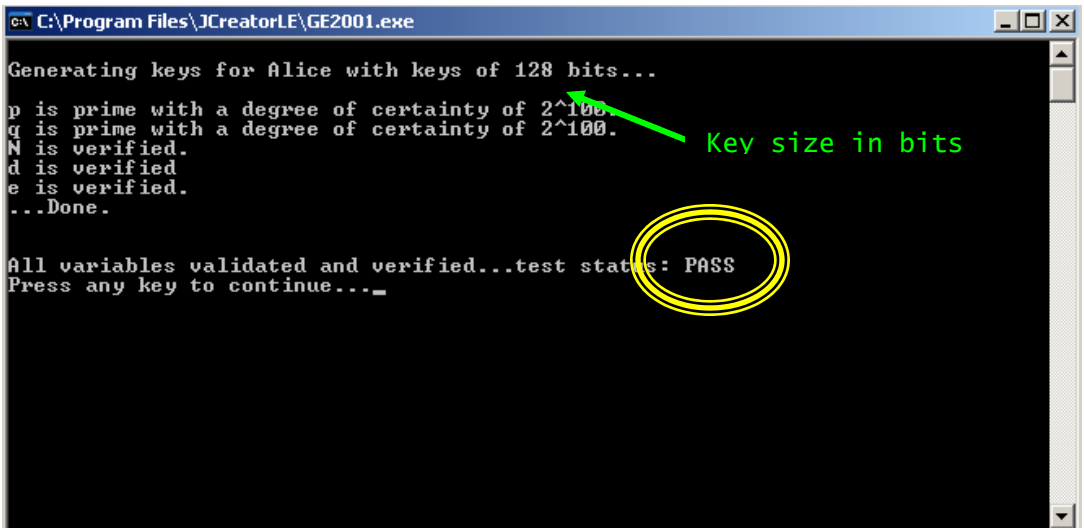
RSA Cryptosystem for ASCII files

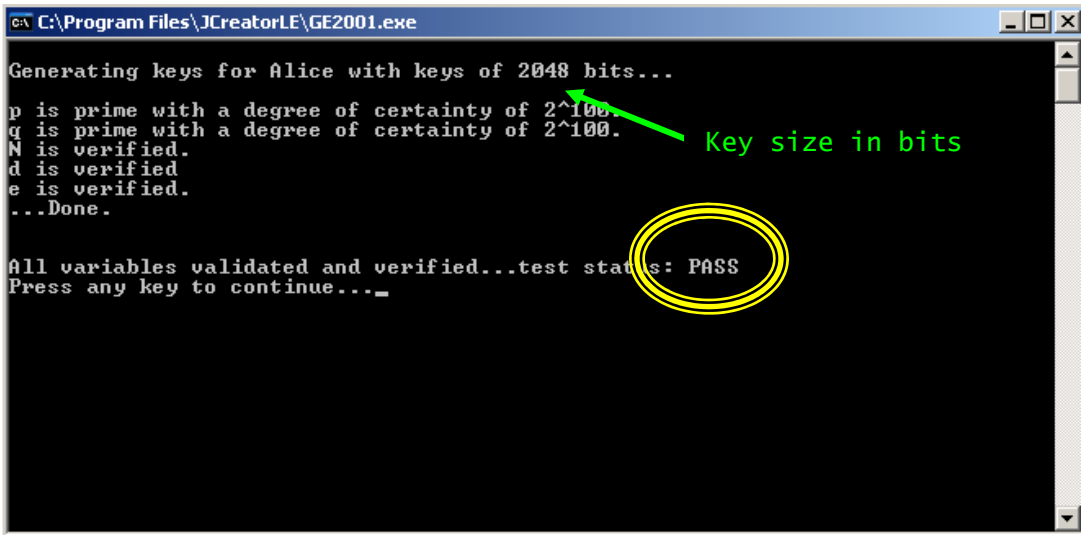
generateKeysTest

For key sizes of 32, 64, 100, 128, 256, 512, 1024, 2048, 4096 and 10,000 bits, run the test 10 different times. (NOTE: key size must be > 20 bits or generateKeysTest will throw exception errors). At least 95 out of these 100 runs, correct and valid values of p, q, N, d, and e must be output. Values of p and q are considered valid if Java.math.BigInteger.isProbablyPrime ( ) returns true with a certainty of 2^{100} when passed in the value of p and q. Values of e, d, and N are verified using other BigInteger methods, which are assumed to be correct.

Results

qpeN™ passed this test with flying colors, returning valid keys for all sizes, on 100% of the runs tested. Examples of the test runs with different key sizes are shown below:





encipher/decipherTest

Due to the broken and divided nature of the process of enciphering, it is impractical to test enciphering and deciphering separately…it would be tantamount to cryptanalyzing the RSA algorithm. The test, will consist, therefore, of comparisons between the plaintext input into the encipher equation and the deciphered plaintext output from the decipher equation. It will be performed on 10 different files in a range of 1KB to 10MB, and 9 out of the 10 times tested, the difference between the two objects must be 0 in order for qpeN™ to pass this test.

Results

qpeN™ passed this test with flying colors, returning identical files on 100% of the valid runs tested. It should be noted that qpeN™ is extremely sensitive to non-ASCII characters in the files given as parameters. Examples of the test runs with different file sizes are shown below: