Math 287 Spring 2023 Test 3

Dr Holmes

April 26, 2023

This is a takehome exam. You are asked not to consult with another human being other than myself in working on this test.

It will be accepted up to 5 pm on Friday May 5.

Please notice that you need to start promptly because problem 2 involves an exchange of email with me.

1. In the privacy of your cryptography lab, you have chosen $p = 29$, $q = 67$ as the primes underlying your RSA key and checked that $r = 5$ is a suitable exponent.

   Describe your public key (the pair of a number N you should know how to compute and your exponent r).

   Verify that your value 5 for r is appropriate (there is a condition you should be able to write down that it has to satisfy).

   Determine your decryption exponent s. Your calculation may use the Eucliean algorithm spreadsheet, but reproduce it on your paper.

   You receive the message $M' = 1166$ from me. Decrypt it. Your calculation may use the modular exponentiation spreadsheet, but reproduce it on your paper.

2. Create an RSA public key of your own. Send me the public information for the key. I will reply with a message: decrypt it and tell me the number I encoded and sent you as a message, and record all work as in problem 1 for creation of the key and decryption of my message on your test paper.

Check that your primes are small enough that the spreadsheet doesn't overflow (by sending yourself a message and making sure that it decrypts correctly), unless you know how to use other software that handles exact arithmetic for big numbers better (Python comes to mind). I do have access to such software, so I should be able to send you a message if you choose to use numbers too large for the spreadsheet; but you also have to be able to decrypt my message.

3. The modulus 1943 has prime factorization (29)(67). Compute $3^{100000} \texttt{mod} 1943$ using the spreadsheet (you may use a screenshot of the spreadsheet or a printout as evidence of this quite large calculation). Then use Euler's theorem (and the lemma about the value of the Euler phi function at products of two distinct primes) to show that this is equivalent to a much smaller power of 3 mod 1943. Evaluate this smaller power of 3 mod 1943 using the spreadsheet and verify that the results are the same.

4. Prove the statement $\lim_{x \to 3}(2x - 1) = 5$. Begin by translating this statement using the official definition of limit, then write out the scratch work and the proof.

   The use of appropriate English words as well as calculations is required. Look at my boardwork for examples of the expected style.

5. Prove the statement $\lim_{x \to 5}(12 - 2x) = 2$. The instructions are the same as on the previous problem. Be careful with properties of absolute value as they relate to negative numbers.

6. Prove the statement $\lim_{x \to 11} x^2 = 121$. The instructions are the same as on the previous problem.