MATH 470 Final checklist

- Once again the last page of the test will have a list of computations that you should use to advantage.
- *Any* of the homework exercises are fair game for the exam.
- The exam will be comprehensive, but will certainly contain the material covered since the last test.
- The exam will have two sections, A and B.
  - The first is short answer - but explanations are **required**. You must show the significant idea before any credit is awarded.
  - Section B is longer questions and you must select 3 from a total of 5. It is imperative here that you pay attention to the descriptive parts. See next pages for some important comments here.
Here is a sample question and below it a student answer. Read it carefully then evaluate how many points it deserves out of 10.

[1] Describe in detail how an RSA public key system is set up and used. [10 points]

Take two large primes $p$, $q$ and multiply them to form $n$.
Take an exponent $e$ that should not be too small.
To send a message $m$, form $m^e \pmod{n}$ and send to Alice.
Decrypt by the formula $c^d \pmod{n}$.
[1] Describe *in detail* how an RSA public key system is set up and used. [10 points]

Take two large primes \( p \), \( q \) and multiply them to form \( n \).
Take an exponent \( e \) that should not be too small.
To send a message \( m \), form \( m^e \mod n \) and send to Alice.
Decrypt by the formula \( c^d \mod n \).

Evaluation of the answers to [1]. Some overview questions:

a. Are you convinced the student knows what they are doing?
b. Are all the relevant pieces included?
c. If you had been given this information the day before we first discussed RSA could you have implemented it just from the answer?
d. How many points?
Evaluation of the answers to [1]. Some overview questions:

a. Are you convinced the student knows what they are doing?

b. Are all the relevant pieces included?

c. If you had been given this information the day before we first discussed RSA could you have implemented it just from the answer?

d. How many points?

First, my answers to the above:

a. Not convinced! I am not sure how much the student knows or understands beyond the fact they have memorized the commonly used symbols for the components.

b. This answer is far from inclusive. Who sends what to whom? Who knows what information? What is public and what is private? Where is the key? All of this is essential in a public key system. Some more detailed points:

   Who picked the $p$, $q$ and $e$? One might assume Alice from the context, but that certainly isn’t stated.

   What about $e$ - we know it cannot be “small” but can it be 1,000,000? Wasn’t something very important missed here?

   We are only told that decryption is by $c^d \pmod{n}$. One might assume that “$c$” is the ciphertext and with a little further assumption and benefit of the doubt, that it is $m^e \pmod{n}$.

   What about $d$ - where did this spring from?

I am sure most of you caught these lapses, so let me ask you the follow-ons:

   would you have been content if they had added: “where $ed = 1$”?

   How about “$d$ is chosen from $ed \equiv 1 \pmod{n}$”? Or “$d$ is chosen from $ed \equiv 1 \pmod{n-1}$”?†

   Of course I hope not, but does one of the above such additions change your answer to question a? How much would it have changed your grading if the correct answer had been given?

   Do you think $\phi(n)$ needs explained?

c. Absolutely not! If this were being described to an educated person with no knowledge of the concept would the central idea have come across? Or, equally germane if this was all that was provided to a programmer with no knowledge of the algorithm would it have been coded correctly?

d. I suspect by now I have convinced you of my answer here already.

   See next page for what I would give.

† I have seen all of these answers.
Zero - and it wasn’t remotely a close call.

What if they had given a correct statement about $d$? Same score. Still too much critical missing information, in particular about what is private/public.

You might say that the student just doesn’t write ideas very well but deserves some/most of the credit for remembering the key symbols and some of the key operations. A senior level class should be considerably beyond this level.