Writing Assignment 1: due by the start of class on Monday, October 6

Your first writing assignment is to write a **careful, complete, clear, and concise** summary of RSA endcoding and decoding.

IMPORTANT NOTE. One of the things that separates "higher" math classes, like this one, from courses like Calculus is that, here, you're expected not to just "know the math," but to communicate it in a cogent (clear, logical, and convincing) way. To this end, in writing up your summary, please follow the guidelines below. Failure to do so will affect your grade.

- Put your name on your work!
- Feel free to work in groups to discuss these problems; your write-ups, however, should be completed individually, in your own words and ideas. If two or more submitted assignments look too similar, I will ask all parties to rewrite their work.
- The finished product should be neat, organized, and legible. If I can't read it, I can't grade it.
- Your summary should be written as though students in this course are the audience.
- Please limit your paper to two pages at the absolute maximum. Being concise is just as important as being complete! If you can do this all in one page, that would be fine too.
- Your paper should be written in complete sentences. (It's okay for complete sentences to contain mathematical symbols, equations, etc. For example, $x = 3$ is a complete sentence!!)
- Your summary should read like a short essay, in paragraph form, rather than a list of bullet points. (It's OK if there are short lists within your paper, but use lists and bullet points sparingly.)
- Use symbols appropriately. For example, don't use "$\rightarrow$" if you mean "$=$" or "$\Rightarrow$." If you don't know which symbol to use, use words instead.
- Please do not deviate from terminology or notation used in class or the RSA notes, unless it's "plain English."
- Use AI if you want, but if you do, it will almost certainly give you something that would look very unfamiliar to students in this class. Make sure you translate things into familiar language, symbols, and ideas.
- If you do use AI or other sources, cite them. You don't need to adhere to any particular reference style. Just something like "I used ChatGPT and the Wikipedia article on RSA." (As with AI, make sure your terminology, notation, and ideas are consistent with what we've learned in class. If not, you'll lose points and/or will be asked to rewrite.)

(over)

- This assignment must be submitted either on paper, in class, before class begins, on the due date, or online through Canvas, before the start of class on the due date. If you are submitting handwritten work online, then you can submit either a scan, or photos, of this work. MAKE SURE YOUR SCANS/PHOTOS ARE CLEAR AND LEGIBLE, or you will lose points.
- If you have the technology and expertise to complete this assignment using a word processing program that is good with math symbols, then feel free to do so. But this is not necessary.
- Here (in no particular order) are some aspects of RSA you might want to consider. You don't need to cover all of these. But a reader should come away with a good idea of the principles, if not all the details, of how RSA encoding and decoding work.

  (a) Successive squaring; what it's needed for and why.

  (b) Euclidean algorithm; what it's needed for and why. (You don't need to prove anything.)

  (c) Numerization.

  (d) Computing remainders mod m.

  (e) Appropriate form for the modulus m.

  (f) $\varphi(m)$.

  (g) How to encode. What conditions need to be met for decodable encoding? (You don't need to prove anything.)

  (h) How to decode. (You don't need to prove anything.)

  (i) Why being able to encode doesn't necessarily mean you can decode, and what else you need to know to be able to do so.

  (j) (Optional; if you want to take it a bit further.) The state of the art: Currently, how large are the numbers (like m, k, p, q) that are used in RSA? Where is RSA actually used? What are the implications of quantum computing for RSA? Etc.