

Instructions for Writing Assignment

GOAL: The purpose of this writing assignment is to demonstrate your understanding of number theory and cryptography by showing that you can express these difficult concepts in plain English. The point is that you can't really accomplish this without fully understanding the mathematics first. In general, explaining your ideas in words in your mathematical and scientific work should force you to clarify your thinking about what you know and what you don't know.

GENERAL GUIDELINES: Finding the right tone in these papers is extremely important. You want to be able to talk seriously about mathematical ideas, but include words to explain them. Your assumed audience should be a fellow student in this class, so you need not start from the very beginning.

Typically in writing-based courses, your papers have a central thesis. This will likely not be the case for these papers. But you should still have an introduction explaining the aim of the paper and outlining what you plan to discuss and you should have a conclusion which not only explains what you've done but also poses directions for future investigation or ideas that you would continue to pursue if you had more time.

TOPICS: Your project is to describe

- (1) Attacks on simple cryptosystems (using shifts and affine maps, digraphs and tri-graphs, etc. even matrices if you find this section of Koblitz interesting)
- (2) Explain RSA with an example (you could even use what you turn in for homework this week, but more generously annotated) making sure to say why the encrypting and decrypting procedure works by including arguments from number theory.
- (3) Select a public key cryptosystem to explore in depth. You could choose RSA for this, but you'd want to go deeper into a discussion of attacks, security, factoring methods and maybe related questions like primality testing. Other public key cryptosystems are discussed in Koblitz. We haven't covered them yet, but we will; remember there are three drafts to this paper, so you can either wait to describe these or begin researching on your own. You can also make appointments with me to talk further about these things.

Here's a list of other cryptosystems you might want to write about:

- (1) Diffie-Hellman cryptosystem
- (2) ElGamal cryptosystem
(We'll cover the above two in the next couple of weeks in our discussion of the discrete log problem)
- (3) Knapsack algorithms (IV.4 in Koblitz)
- (4) Elliptic curve cryptosystems (Chapter VI in Koblitz)

And then related to RSA you might talk about factoring algorithms such as

- (1) Pollard's ρ (rho) method
- (2) Pollard's $p - 1$ method
- (3) the quadratic sieve method
- (4) Lenstra's elliptic curve factorization
- (5) the number field sieve

or about primality testing and Carmichael numbers, etc.

I'd like to encourage creativity on these assignments, so let me stress that any careful discussion of cryptography which includes such a public key method is valid.

FORMATTING, ETC.: While there is no length requirement, it seems to me that a good paper would take 8 to 10 pages to explain. For the final drafts, typed papers are greatly preferred. They should be self-contained rather than referring to diagrams which are not included. Also remember that I am placing weight on your better performances in the class, so this is a chance to do something good to give me something to think about when preparing grades, especially if you haven't performed as well as you would like midterms and homework. No grade will be given on these until at least the second draft is turned in. However drafts must be turned in at all stages as part of the revision process.

WHAT TO DO FOR THE FIRST DRAFT: Simply put, you can do as much or as little as you want, but keep in mind that the more substantive the draft, the better we can comment on what needs to be done. At least, you could describe the elementary methods and RSA and possibly think about what you might like to work further on for your public-key portion.