Encryption/Decryption with Matrices

Mark McKelvy
CMPS352

Abstract

In this project, I want to try to understand simple encryption and decryption better. Therefore, I plan to use MATLAB to help me see how this process works in order to better visualize what is happening. The inspiration for this idea had its roots early on when I took a linear algebra class in high school. My teacher glossed over the use of matrices in simple cryptography. With my recent introduction to MATLAB, I have become inspired to research into this topic further and create something that can actually do encryption and decryption, using the things I have learned in this class and my linear algebra class, and things I will learn from working on this project. I have referenced the class textbook by Cleve Moler [Mol01] because it also has a brief introduction to this same process. I hope to use the description within the text as a springboard to something a little more advanced, but along the same lines. At this point my research will begin with chapter 1, section 5 of Moler. This will be a necessary stepping stone towards something better. At this point it is my understanding that this kind of cryptography involves a lot of matrix multiplications and inverses, and I hope to learn what can make this cryptography stronger or weaker. I would like to know whether the amount of characters represented makes a difference, as well as the matrix size, or other matrix factors that have yet to be explored.

References

[Mol01] Cleve Moler. *Numerical Computing with MATLAB*. SIAM, 2004.