Derek Ditch
Linear Algebra I

10/10/03
Insall, Matt Ph.D.

Cryptology is the union of the two fields of cryptography and cryptanalysis.[2] Cryptography is the art of securing a message through an insecure medium, such as an encoded letter in the US mail system. Cryptanalysis is the art of breaking this security when one is not cleared for access. Cryptology has been an important tool to government and military officials since prehistoric times. Writing was the simplest means of cryptology because few people understood it. It quickly evolved into some of the more advanced techniques we use today for national security and bank transactions.

There are two major branches of cryptography, coding and ciphering. Coding involves substituting words, phrases, or sequences with other words, phrases, or sequences in a one-to-one relationship. This is a very simple method and often easy to reverse. A more sophisticated method later arose, called ciphering.[2] This is when a letter, word, or sequence is replaced with a process, often mathematical, which will yield a value based on a key.

A fairly strong cipher is the Hill cipher. This is a polygraphic cipher that uses two or more letters per group. This cipher was the first to successfully apply linear algebra to a polygraphic cipher. Using this method, a change by one or two letters in the text will completely change the cipher text, or the encrypted message.[1] This makes Hill ciphers especially difficult to "crack" or cryptanalyze. Cracking a Hill cipher generally takes a large amount of captured cipher text.

Hill ciphers heavily rely on modular arithmatic and linear transformations. The algorithm is fairly simple to implement. First, choose an alphabet of *m* characters. It is easier to find a valid key if *m* is a prime number. Many alphabets will contain the standard letters plus punctuation and a character to represent a space. Next, select a key. The key is an *n x n*

matrix containing any sequence of numbers so that, each value is in the range [0, *m*-1], and the resulting matrix is invertible modulo *m*. This is why it is easier if *m* is a prime number. This will be called matrix A. The next step is to assign a unique value to each character of the alphabet with a value of 0 to *m*-1. Substitute the character's value for each character in the text string. Break this string of values into a series of vertical vectors of *n* rows each. Append these vectors to create a matrix, in the proper sequence. This will be matrix B. Multiply matrix A by matrix B to get matrix C. Matrix C should then be reduced to the least congruent matrix modulo *m*. By seperating matrix C into ciphertext vectors, the values can be reordered into their proper sequence. Substitute the characters from the alphabet to with their corresponding numbers. The result is a Hill cipher ciphertext.[1]

The only way to decipher the text, is to know the inverse of the original key. This is why it is of utmost importance to choose an invertible matrix. Otherwise you have just created a string of garbage. To decipher the text, find the inverse of A modulo *m*. The modulo *m* operation keeps the values in the correct vector space. This is the decipher key. Apply the same algorithm as stated above using A^{-1} in place of A to get the original text.

References

[1] Murray Eisenberg, *Hill ciphers and modular linear algebra*, mimeographed notes, University of Massachusetts, 1998, 19 pages.

[2] François Morain, *A history of cryptology*, Algorithms seminar, LIX École polytechnique, 1997, 2 pages.