Lecture 25– The Hill Cipher

The Hill Cipher is an example of a cipher where blocks of letters are manipulated rather then of individual letters. A previous example of such a cipher was the anagram cipher in which blocks of 2 or more letters were rearranged.

A Hill Cipher starts with H_n , an ***n***-by-***n*** matrix of integers. Since we are working in MATLAB ASCII, the matrix will have a modulus of 95. We then divide a clear text into blocks of ***n*** letters each. If the length of the clear text is not divisible by ***n***, spaces must be added to the end of the text. We convert each block of letters to ASCII and, as before, subtract 32 to create a vector of integers that contains values between 0 and 94. We now encrypt the first block of clear text integers $[T_1, T_1, \ldots, T_n]$ by multiplying by the matrix H_n (mod 95).

For example, consider $H_3 = \begin{bmatrix} 32 & 25 & 34 \\ 91 & 16 & 76 \\ 43 & 21 & 12 \end{bmatrix}$ and the clear text "cat", which after conversion becomes [67 64 84]. Now perform the cipher operation:

$$\begin{bmatrix} 32 & 25 & 34 \\ 91 & 16 & 76 \\ 43 & 21 & 12 \end{bmatrix} \begin{bmatrix} 67 \\ 65 \\ 84 \end{bmatrix} mod\ 95 = \begin{bmatrix} 70 \\ 31 \\ 29 \end{bmatrix}.$$

The resulting encrypted text is "f?=". To decrypt the text we multiply the encrypted text by the inverse of H_3.:

$$\begin{bmatrix} 59 & 91 & 64 \\ 29 & 43 & 73 \\ 7 & 42 & 23 \end{bmatrix} \begin{bmatrix} 70 \\ 31 \\ 29 \end{bmatrix} mod\ 95 = \begin{bmatrix} 67 \\ 65 \\ 84 \end{bmatrix}.$$

Note the inverse above is in mod 95, i.e:

$$\begin{bmatrix} 32 & 25 & 34 \\ 91 & 16 & 76 \\ 43 & 21 & 12 \end{bmatrix} \begin{bmatrix} 59 & 91 & 64 \\ 29 & 43 & 73 \\ 7 & 42 & 23 \end{bmatrix} mod\ 95 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The general theory for determining in modular inverse of matrices is beyond the scope of this project; however, I will offer some observations:

- The modular matrix can consist only of integers between 0 the modular value minus 1 (i.e. for mod 95, the matrix will have integers from one to 94.)
- If the determinant of the matrix equals zero, the matrix is not invertible.
- If the determinant of the matrix shares a common factor with the modulus, the matrix is not invertible. I.e. for mod 95, the determinant can not be a multiple of 5 or 13.
- IF THE MATRIX IS NOT INVERTIBLE, YOU CAN NOT DECRYPT THE MESSAGE!!

In order to assist you in finding modular inverses of matrices, us the following applet found at: http://www.eecg.utoronto.ca/~bradel/projects/cryptography/index.html. The following inputs to this applet apply to for this project:

- Cipher Size: The dimensions of the encryption matrix.
- Lower Bound: 0
- Upper Bound: 94 (for mod 95)
- First Value: any integer … does not affect inverse.
- Encryption Array: The values of the array. Can be written as a line of numbers with spaces in-between.