Project: Cryptography

General Information. The study of encoding and decoding secret messages is called *cryptography*. Codes are called *ciphers*, encoded messages *ciphertext*, and uncoded messages *plaintext*. The process of converting from plaintext to ciphertext is called *enciphering*, while the reverse is called *deciphering*. In this project you will learn about substitution ciphers and a special kind of substitution cipher sometimes called a *Hill cipher*. Hill ciphers use linear algebra.

Key Words. Enciphering, deciphering, modular arithmetic, linear transformations, Hill n-cipher, digraph.

References. Look for books on mathematical approaches to cryptography. For additional texts on modular arithmetic, you can look at a basic number theory book.

Problems. In the following problems, assume the use of the usual 26 letter alphabet with A=0 and Z=25, unless otherwise specified.

(1) You intercept the message "SONAFQCHMWPTVEVY," which you know was enciphered using a Hill 2-cipher. An earlier statistical analysis of a long string of intercepted ciphertext revealed that the most frequently occurring ciphertext digraphs were "KH" and "XW" in that order. You take a guess that those digraphs correspond to "TH" and "HE," respectively, since those are the most frequently occurring digraphs in most long plaintext messages on the subject you think is being discussed. Find the deciphering matrix, and read the message.

(2) In order to increase the difficulty of breaking your cryptosystem, you decide to encipher your messages using a Hill 2-cipher by first applying the matrix $\begin{pmatrix} 3 & 11 \\ 4 & 15 \end{pmatrix}$ working modulo 26 and then applying the matrix $\begin{pmatrix} 10 & 15 \\ 5 & 9 \end{pmatrix}$ working modulo 29. Thus, while your plaintexts are in the usual 26 letter alphabet, your ciphertexts will be in the alphabet with 0-25 as usual and blank=26, ?=27, and !=28.
   (a) Encipher the message "SEND".
   (b) Describe how to decipher a ciphertext by applying two matrices in succession, and decipher "ZMOY".
   (c) Under what conditions is a matrix with entries modulo 29 invertible modulo 29?