MATH 587/CSCE 557 - SUMMARY OF CLASS, 1/25/07

I explained how the word 'alphabet' is often used in the literature in place of 'cipher' and pointed out that a cryptosystem consists of a collection of ciphers (one for each key). There are other names for ciphers, e.g. a shift cipher is sometimes called a direct standard alphabet. We will not use this other terminology.

The shift and affine ciphers are 'monoalphabetic' ciphers, i.e. block ciphers with blocks of length 1. The most general kind of monoalphabetic cipher is a substitution cipher. This cryptosystem has $P = C = \mathbf{Z}_{26}$ and K consists of all permutations of this set. The goal of modern block ciphers is to simulate random permutations.

A block cipher with blocks of length > 1 is called polyalphabetic. The most famous is the Viginère cipher. Encryption is performed by using a sequence of shift ciphers. You pick a key word, e.g. CRYPTO, and write CRYPTOCRYPTOCRYPTO... below your message to be encrypted. Then add the 1st letters of both rows together, then the 2nd letters of both rows, and so on. (Addition is done by converting the letters to elements of $\mathbf{Z}_{26}$.) To decrypt, take the complementary word to the key word, i.e. C gets replaced by Y since $2 + 24 = 26$, R replaced by J since $17 + 9 = 26$, ... so we get YJCLHM. Write YJCLHMYJCLHMYJCLHM... below the message to be decrypted and add just like before. Viginère ciphers can be broken (see later cryptanalysis) but are still used from time to time in modern systems.

For Hill ciphers, the key is a square matrix M. If M has n rows and n columns, the message to be encrypted is broken into blocks of length n. To encrypt a block, consider it as a column vector $x_1, ..., x_n$ of elements of $\mathbf{Z}_{26}$ and compute M times this vector. Whenever you get numbers outside 0 to 25, reduce mod 26. Then turn these numbers back into letters. To decrypt a block, multiply it by the inverse matrix M^{-1}. If $n = 2$, say $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $M^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Here $(ad-bc)^{-1}$ indicates the reciprocal of $ad-bc \pmod{26}$, and we get a legitimate cipher only when $ad - bc \in \mathbf{Z}_{26}^*$.