MATH 587/CSCE 557 - SUMMARY OF CLASS, 1/23/07

Class was cancelled on Thursday, 1/18/07, because the university opened late because of bad weather. Today, after handing out copies of the course syllabus and the first homework (which had been posted online on Wednesday), I recapped what a cryptosystem consisted of (set of plaintexts, set of ciphertexts, set of keys, and encryption and decryption functions for each key k such that $d_k(e_k(x)) = x$).

I recalled the example of shift ciphers and then showed how, given a word encrypted by a shift cipher, you can (basically by trying all 26 keys) find the original word (i.e. plaintext) and the key used to encrypt. (Our first go at cryptanalysis.) Be careful - if shifting by k turns the ciphertext into a sensible English word, the key used to encrypt is $-k$ or $26 - k$, rather than k itself. Things to note - systems with few keys are weak; we're helped by the fact that strings of letters that form words are relatively rare as a proportion of all possible strings of letters.

I then introduced affine ciphers. Here $P = C = \{0, 1, 2, ..., 25\}$ (identified with $A, B, .., Z$ as usual) and our encryption functions are of the form $e_k(x) = ax + b$ (mod 26). Some choices of a (e.g. $a = 13, 4$) don't lead to legitimate encryption functions since two letters get encrypted to the same thing which then can't be decrypted. Considering possible decryption functions $d_k(y) = cy + d \pmod{26}$, we saw that we want to pick c, d such that $ca = 1 \pmod{26}$ and $d = -cb \pmod{26}$, in order that $d_k(e_k(x)) = x$ for all x.

This is why certain a don't give legitimate cryptosystems. $ca = 1 \pmod{26}$ doesn't always have a solution. In fact, it does if and only if $\gcd(a, 26) = 1$, so a is in $\mathbf{Z}_{26}^* := \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$. Then c is called the reciprocal of a (mod 26).

Thus, affine ciphers have $P = C = \{0, 1, 2, ..., 25\}$, $K = \{(a, b) \mid a \in \mathbf{Z}_{26}^*, b \in \mathbf{Z}_{26}\}$, $e_k(x) = ax + b \pmod{26}, d_k(y) = cy + d \pmod{26}$, where c, d are calculated from a, b as above. There are $12 \times 26 = 312$ keys so these aren't as weak as shift ciphers - we'll discuss cryptanalysis of them later.