## MATH 587/CSCE 557 - SUMMARY OF CLASS, 4/10/07

The 2nd midterm was handed back, the score distribution given, and the answers explained (they're posted online).

Digital signatures using RSA were discussed. Suppose Alice wants to send her signature to Bob. If her public key is $(N, e)$ (note hers not Bob's), then she knows the corresponding decryption exponent $d$. If she picks some $x$ and computes $s = x^d \pmod N$, she can send $x, s$ to Bob (but an impersonator cannot). Bob can then check her signature by computing $s^e \pmod N$, which should come out as $x$. We discussed traps to avoid and use of hash functions to shorten messages.

Next we went on to modern block ciphers. For each key $k$, this consists of an invertible function $B_k$ from the set of bit strings of length $m$ to itself. We need $m$ to be large (otherwise it's a substitution cipher on a small alphabet and we have ways to attack that - this also applies if the messages come from a low entropy set) and also the set of keys to be large (otherwise we can exhaustively try decoding with each until we get the right one). The encryption functions shouldn't be linear or affine (otherwise Hill or Vigenere cryptanalysis can be used).

We discussed modes of operation. Suppose we break up the message into blocks, each of $m$ bits, say $x_1, x_2, ....$ In codebook mode, the ciphertext is simply $y_1, y_2, ...$ where $y_i = B_k(x_i)$. In block chaining, $y_i = B_k(y_{i-1} + x_i)$ where $y_0$ is given. This has the benefits of not encoding repeated blocks the same way and of propagating transmission errors so they won't be overlooked. In cipher feedback mode, $y_i = x_i + B_k(y_{i-1}$, again with a given $y_0$.

Finally we discussed what to do with short blocks, i.e. suppose the message does not have length exactly divisible by $m$ but that there is a block $x_n$ at the end of length $m' < m$. One possibility is to pad, i.e. fill in the remaining bits with random bits. Another is ciphertext stealing, where if the first $m'$ blocks of $B_k(x_{n-1})$ are $\alpha$ and the remaining $m - m'$ bits are $\beta$, you set $y_{n-1} = \alpha$ (a short block) and $y_n = B_k$ of the block made from $\beta$ followed by $x_n$.