MATH 587/CSCE 557 - SUMMARY OF CLASS, 4/26/07

Note that the final will be on Weds, May 2, at 9am in the usual room. Everyone must attend. There will be a review session at 5pm, Tues, May 1, in LC 312. I shall be in my office (LC 427) from 9am to 2:30pm on Tues, May 1, ready to answer questions. If you have questions before then, please email me.

I went over the problems from HW 10 and over some logistical matters related to the final. Then Roopa gave a 10-minute presentation on attacks on RSA and Deepika gave a 10-minute presentation on password encryption for the Linux operating system. Finally teaching evaluations were handed out.

To review for the final, please look through your notes and the posted summaries. Here's a brief summary of the main topics: classical cryptosystems (shift, affine, substitution, Vigenere, Hill), modular arithmetic, kinds of attack (chosen-plaintext, known-plaintext, ciphertext-only), frequency analysis, maximizing correlation, index of coincidence, Kasiski's attack, one-time pad, entropy, redundancy, linear feedback shift registers, public-key cryptography, RSA encryption/decryption, squaring and multiplying, factoring via quadratic sieve, Diffie-Hellman key exchange, operating modes, Feistel ciphers, DES, birthday attack, AES, digital signatures, cryptographic hash functions.