MATH 587/CSCE 557 - SUMMARY OF CLASS, 4/24/07

We covered flipping coins by telephone. Amber picks two large primes p, q, which (mod 4) are both 3. She keeps them secret and sends $N = pq$ to Rob. He picks a random integer x and sends $y = x^2 \pmod N$ to Amber. In fact y has 4 square roots $\pmod N$, $\pm x$ and two others. Amber can compute all four and she chooses one (the flip) and sends it to Rob. If Rob receives $\pm x$, then Rob says she wins, whereas if Rob receives anything else, he says he wins. If Amber challenges this, Rob can use the fact that he knows all the square roots of $y \pmod N$ to find the factors of N and send these to Amber to prove that he didn't cheat. If Amber sent $\pm x$, Rob is none the wiser and cannot factor N (which is why p, q should be large).

If the other square roots $\pmod N$ of y are $\pm z$, then if Rob knows x and z, he simply computes $\gcd(x - z, N)$ by Euclid's algorithm to get a factor of N. The reasoning is the same as for why the quadratic sieve works. As for Amber computing the four square roots, she computes $\pm y^{(p+1)/4} \pmod p$ (this is why $p \mod 4$ should be 3), which using Fermat's little theorem has square $y \pmod p$. Likewise, $\pm y^{(q+1)/4} \pmod q$ has square $y \pmod q$. Each of the four choices of sign leads by the Chinese Remainder Theorem to a square root $\pmod N$ of y.

Then Ashley gave a 10-minute presentation on Huffman encoding and Keisha gave a 10-minute presentation on steganography. My office hours today will be 1:30-2 and 3-3:30 because of a clash. There will be a review session next Tuesday from 5-6 in 312 LeConte. I will also be available that day until 2:30pm in my office. Students are strongly encouraged to come and see me before the final if they have questions.