MATH 587/CSCE 557 - SUMMARY OF CLASS, 4/19/07

I advertised Alice SIlverberg's IMI Distinguished Lecture on "Diffie-Hellman and beyond" later that day. I then talked about authentication methods, attacks on them (dictionary attacks), and refinements (salting, where you use a family $e_s(x)$ of encryption functions). I reminded the class of using RSA (or other public key systems) for authentication. Then I went over the solutions to homework 8.

Then we discussed cryptographic hash functions h and their desired properties. We want h to send a large set to a small set, to be easily calculable, to be non-invertible (given y it's hard to find x such that $h(x) = y$), and avoid collisions (it should be hard to find x, x' such that $h(x) = h(x')$). A method using finite state automata was given. Suppose Q is a finite set of states and X a set of symbols. Let $\delta : Q \times X \to Q$ be a finite state automaton. Suppose we have an initial state q_0. Break a given message x into $x_0, x_1, ..., x_n$. Let $q_i = \delta(q_{i-1}, x_{i-1})$ and successively compute $q_1, q_2, ..., q_{n+1}$. Set $h(x) = q_{n+1}$. This is sometimes called a message digest. Popular cryptographic hash functions include MD4, MD5, SHA, and SHA-1, but all have come under doubt in the last three years because of collision-producing attacks. In these Q is $\{0,1\}^{128}$ and X is $\{0,1\}^{512}$.

I then talked a little bit about flipping coins on the telephone, which will be completed next time.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX