MATH 587/CSCE 557 - SUMMARY OF CLASS, 4/17/07

I repeated the quick description of DES (up to permutations) and then spoke of its history. It became the official data encryption standard in 1977 and did pretty well for 20 years but gradually a 56-bit key started to seem too short. In 1997 a challenge to crack DES was met by Rocke Verser in 5 months using a bruteforce distributed search, successful after 25% of the key space was searched. In 1998, DES Challenge II was met in 39 days after 85% of the key space had been searched. Soon thereafter the Electronic Frontier Foundation built a DES Cracker that took 4.5 days on average to crack DES.

One suggested remedy was multiple encryption, i.e. take two keys k_1, k_2 and let $e_k(x) = e_{k_2}(e_{k_1}(x))$ and $d_k(y) = d_{k_1}(d_{k_2}(y))$. Since "DES is not a group", meaning that unlike e.g. Vigenere systems, composing two DES ciphers does not (necessarily) give a single DES cipher, this could perhaps lead to increased security. The problem is that there is another attack, the birthday attack (think of how it is better than even odds that in a group of 23 people, two have the same birthday). The idea is, given two plaintext/ciphertext pairs $(x, y), (x', y')$, to save for each DES key $(e_k(x), e_k(x'), k)$ and $(d_k(y), d_k(y'), k)$. There are 2^{57} such triples. Once you find a pair of triples where the first two entries match, i.e. $e_{k_1}(x) = d_{k_2}(y)$ and $e_{k_1}(x') = d_{k_2}(y')$, then $e_{k_2}(e_{k_1}(x)) = y$ and $e_{k_2}(e_{k_1}(x')) = y'$, and so (k_1, k_2) is a candidate for the key. It turns out that the chance of an incorrect match is about 2^{-16}, so we can be confident we have the key. As a result, triple DES (3DES) was instead used, with $e_k(x) = e_{k_1}(d_{k_2}(e_{k_1}(x)))$, but there are still weaknesses.

In 1997, NIST announced a competition to start afresh and come up with an encryption standard. In 1998, 15 algorithms were entered, and out of 5 excellent finalists, Rijndael was chosen to become, in 2002, the new Advanced Encryption Standard (AES). It satisfied various requirements, such as that it allows key sizes of $128, 192$, or 256 bits, blocks are 128 bits and can be used in ECB (electronic codebook), CBC (cipher block coding), or CFB (cipher feedback) modes, it works on 8-bit processors (smart cards) or 32-bit processors (PC's), and has speed and resistance to cryptanalysis.

AES consists of 10 rounds of ByteSub transformations, ShiftRow transformations, MixColumn transformations, and AddRoundKey. The bits form 8-bit bytes, which are viewed as elements of the finite field $GF(256)$. Nonlinearity, to resist various attacks, is built in the ByteSub transformations and the key schedule via an S-box which comes from inversion in $GF(256)$. This is more natural than the S-boxes in DES, removing tampering fears but opening up fears of algebraic attacks.

I mentioned IDEA and Skipjack, and then mentioned some other uses of cryptography such as authentication, integrity, and commitment. An example of password encryption via a one-way function was given. Suppose your password is x. Using a public large prime p and integer $g > 1$, $e(x) = g^x \pmod p$ is stored by the computer in the clear. Anyone wanting to impersonate you will have to compute the x that produces this $e(x)$, which is hard.