MATH 587/CSCE 557 - SUMMARY OF CLASS, 3/22/07

I reviewed the RSA cryptosystem, gave an example, and then justified why encryption followed by decryption gets you back to where you started.

For the example, we needed to compute $x^e \pmod N$. (Recall that $a \pmod N$ means the remainder on dividing a by N.) By writing e in binary, i.e. as a sum of powers of 2, it's enough to find $x^2 \pmod N, x^4 \pmod N, x^8 \pmod N, \ldots$ These can be computed by repeatedly squaring and reducing $\pmod N$ as we go along. So, for example, having computed that $7^2 \pmod{11} = 5$ (since 5 is the remainder on dividing 49 by 11), we can compute $7^4 \pmod{11} = 5^2 \pmod{11} = 3$.

The point is that to work out $ab \pmod N$, we just need to multiply $a \pmod N$ and $b \pmod N$ and take the answer $\pmod N$.

Writing e as a sum of powers of 2 means that we can quickly compute $x^e \pmod N$, in fact in about $2\log_2(e)$ steps. This is good - we want the system to take little time for implementation (but a lot of time to be cracked).

Now encrypting followed by decrypting takes x to $D(E(x)) = x^{de} \pmod N$, where $N = pq$ and $de = 1 + k(p-1)(q-1)$ for some integer k. So let's look at $D(E(x)) = x^{1+k(p-1)(q-1)} \pmod N$.

I claim that $D(E(x))$ is x plus a multiple of p. There are two cases: If x is divisible by p, this is immediate since powers of x are also multiples of p. If x is not divisible by p, then Fermat's Little Theorem says that x^{p-1} is 1 plus a multiple of p, say $x^{p-1} = 1 + cp$ for some integer c. Then $x^{1+k(p-1)(q-1)} \pmod N = x(1+cp)^{k(q-1)} \pmod N = x(1 + k(q-1)cp + \text{other multiples of } p) \pmod N$, which is x plus a multiple of p, as claimed.

Likewise, making the same argument with q in place of p, $D(E(x))$ equals x plus a multiple of q. So $D(E(x)) - x$ is a multiple of p and of q, whence it's a multiple of $N = pq$. Since $0 \leq x \leq N-1$, $D(E(x)) \pmod N = x$.