Math 445 Number Theory

September 13, 2004

Public key cryptosystem vulnerabilities:

(1) The public key (N, e) is public! Anyone can spend any amount of time breaking it (by factoring N), without waiting for cyphertext to be intercepted. Which is why we want N to be so hard to factor....

(2) If someone can guess what message (or which 1,000,000 messages) you might be sending, they can compute what cyphertext $B = A^e \pmod N$ would correspond to that message, effectively reading the message A without knowing the secret key d.

On a lighter note, the analysis we have developed can shed light on *repeating decimal expansions of fractions.*

A number like $\dfrac{1}{13} = 0.076923076923\ldots = 0.\overline{076923}$ has a repeating pattern, every 6 digits (in this case). What this means is that

$$\frac{1}{13} = \frac{76923}{10^6} + \frac{76923}{10^{12}} + \frac{76923}{10^{18}} + \cdots = (76923)\left(\frac{1}{10^6} + \left(\frac{1}{10^6}\right)^2 + \left(\frac{1}{10^6}\right)^3 + \cdots\right) = \frac{76923}{10^6 - 1}$$

The *period* of the decinal expansion is 6, because $10^6 - 1 = (13)(76923)$, i.e., $10^6 \equiv 1 \pmod{13}$, and 6 is the smallest positive number for which this is true. Borrowing some terminology from group theory, we say that the *order* of 10, mod 13, is 6, and write $\mathrm{ord}_{13}(10) = 6$; it is the smallest positive power of 10 which is $\equiv 1$ mod n. The definition of $\mathrm{ord}_n(a)$ is similar.

In general, $\mathrm{ord}_n(a)$ makes sense only if $(a, n) = 1$; then, by Euler's Theorem,

$$a^{\Phi(n)} \equiv 1 \pmod n$$

where $\Phi(n) =$ the number of integers b between 1 and n with $(b, n) = 1$. So there is a smallest such power of a . Conversely, if $a^k \equiv 1 \pmod n$, then $a \cdot a^{k-1} + n \cdot x = 1$ for some x, so $(a, n) = 1$.

Since $a^k, a^m \equiv 1 \pmod n$ implies $a^{(k,m)} \equiv 1 \pmod n$, if $(a, n) = 1$ then $\mathrm{ord}_n(a) | \Phi(n)$. So we can test for the $\mathrm{ord}_n(a)$ by factoring $\Phi(n) = p_1^{k_1} \cdots p_r^{k_r}$. We know $a^{\Phi(n)} \equiv 1$; if we test each of $a^{\Phi(n)/p_i}$ and none are $\equiv 1$, then $\mathrm{ord}_n(a) = \Phi(n)$. If one of them is $\equiv 1$, then $\mathrm{ord}_n(a) | \Phi(n)/p_i$; continuing in this way, we can quickly determine $\mathrm{ord}_n(a)$.

One question about periods that still remains unsolved is : are there infinitely many n for which $\mathrm{ord}_n(10) = \Phi(n)$? The conjectured answer is "yes"; in fact, Gauss conjectured that there are infinitely many primes p with $\mathrm{ord}_p(10) = p - 1$.