Math 445 Number Theory

September 10, 2004

Public Key Cryptosystems: The idea behind a cryptosystem is to provide a method of encoding a message so that only the person intended to receive it can recover the original message. Public key systems take the added step of publishing the encoding method for all to see.

The RSA cryptosystem is a public key cryptosystem which uses exponentiation mod N as its encoding and decoding method. To build it, we need a pair of large (distinct) primes p, q and a number e with $\gcd(e,(p-1)(q-1)) = 1$. We set $n = pq$, and publish n and e . Privately, we also find (via the Euclidean algorithm) a number d (and x) satisfying $de - x(p-1)(q-1) = 1$. We then keep d secret (and throw away our calculations, including the values of p and q).

To send us a message, the text is first converted into a string of numbers, using some standard procedure (e.g., use the ascii character codes for the symbols in the message), which are then cut into pieces each having fewer digits than n. Let A be one such string. You then compute, using my public key, the value

$$B = A^e \pmod{n}$$

and send me the number B. Then I compute

$$B^d = (A^e)^d = A^{ed} = A^{x(p-1)(q-1)+1} = A(A^{(p-1)(q-1)})^x = A1^x = A \pmod{n}$$

since $A^{(p-1)(q-1)}$ is $\equiv 1$ mod p and q, so is $\equiv 1$ mod n (since $\gcd(p,q) = 1$) .

The security of this system lies in the fact that, to the best of our knowledge, the message A cannot be recovered from the cypher B, without knowing d, which requires you to know $(p-1)(q-1)$ (to find it the way we did), which requires you to know p and q, which requires you to factor n. So its strength lies in the fact that (to the best of our knowledge) finding the prime factors of a large number is hard, especially when the primes are large!

To make things more interesting, if you also have a public key system, (n_1, e_1, d_1), then you can (after we have agreed to do this...) apply a two-step process to the message; take the message A and compute

$$B = A^{d_1} \pmod{n_1} \text{ , and then compute } C = B^e \pmod{n},$$

and send me C. I then compute

$$B = C^d \pmod{n} \text{ , and } A = B^{e_1} \pmod{n_1} \text{ ,}$$

to recover the original message. This message, just because I can read it, tells me that only you could have sent it (because only you know d_1). The message can only be read by me, and could only have been sent by you.