The RSA Algorithm

This is meant to be a quick sketch of the RSA algorithm so that you have an idea of how and why it works.

1. Select two large prime numbers p and q. Compute $n = pq$.

Typically these are fairly large. See after the next step.

Example: use $p = 419$ and $q = 541$. Then $n = 226,579$.

2. Compute $n = pq$ and $m = \phi(n) = (p-1)(q-1)$.

The company RSA suggests that by the year 2010, for secure cryptography one should choose p and q so that n is 2048 bits, or $2^{2048} \approx 3 \times 10^{616}$. This is a large number, and a bit more than your calculator can probably handle easily.

Our example: $m = \phi(226,579) = (419-1)(541-1) = 225,720$.

3. Pick an integer e relatively prime to $m = (p-1)(q-1)$.

To decrypt an encrypted message A, we will be computing $A^e \bmod n$.

Our example: we'll choose $e = 2737$.

4. Compute d, the multiplicative inverse of e modulo $\phi(n) = m$

That is, we're computing d so that $ed \equiv 1 \bmod m$. We'll be using d to encrypt a message a to A; again, we'll be computing $A \equiv a^d \bmod n$. The idea is d and e invert each other, so that

$$\left(a^d\right)^e = a^{de} \equiv a \bmod n.$$

Why does this work? Since $de \equiv 1 \bmod m$, we have $de = 1 + km$ for some integer k. That is, $a^{de} = a^{1+km} = a^1 \cdot (a^m)^k$. But Euler's theorem says that $a^{\phi(n)} \equiv 1 \bmod n$, so we get

$$a^{de} = a \cdot \left(a^{\phi(n)}\right)^k \equiv a \cdot 1^k = a \bmod n$$

Our example: our value of d is $d = 46513$. I computed this by using the Euclidean algorithm to compute $\gcd(e, m)$, from which I got the equation

$$1 = 46513 * 2737 + -564 * 225720$$

This says that $46513e \equiv 1 \bmod 225720 = m$.

5. Encrypt with "Public Key" $P = (e, n)$, decrypt with "Secret (Private) Key" $S = (d, n)$. Keep $m = \phi(n)$ secret as well.

The basic steps of encryption / decryption are:

(1) Convert text message to a numerical message a.

(2) Encrypt a to $A \equiv a^e \bmod n$. Now A (the encrypted message) is safe from eavesdropping.

(3) Decrypt A to $a \equiv A^d \bmod n$.

Note that the encryption / decryption process is entirely reversible. That is, if someone encrypts something with your Public Key $P = (e, n)$, then to decrypt it one needs your Secret Key $S = (d, n)$.

6. Encryption / Decryption Using Our Example: Two problems: first,

(a) Decrypt the message `128661`. This will produce a number.

Convert this number, two digits at a time, to text by assuming `01=A`, `02=B`, `03=A`, and so on up to `26=Z`, and `27`=space. (For this example we won't use anything but letters and spaces.) For example, the number `030120` would be `CAT`.

Alternate problem: using $p = 113$ and $q = 151$. This will make the computation easier. The Public Key is now chosen to be $P = (e, n) = (12587, 17063)$ and the encrypted message is `14747`. (This is the same message as before, it's just that the calculations are simpler.)

(b) Encrypt your initials (or any three letters) using this public key.