Numerical Example of RSA

Gilles Cazelais

To generate the encryption and decryption keys, we can proceed as follows.

- 1. Generate randomly two "large" primes p and q.
- 2. Compute n = pq and $\phi = (p-1)(q-1)$.
- 3. Choose a number e so that

$$gcd(e, \phi) = 1.$$

4. Find the *multiplicative inverse* of e modulo ϕ , i.e., find d so that

$$ed \equiv 1 \pmod{\phi}.$$

This can be done efficiently using Euclid's Extended Algorithm.

The encryption public key is $K_E = (n, e)$ and the decryption private key is $K_D = (n, d)$.

The encryption function is

$$E(M) = M^e \mod n.$$

The decryption function is

$$D(M) = M^d \bmod n$$

These functions satisfy

$$D(E(M)) = M$$
 and $E(D(M)) = M$

for any $0 \le M < n$.

Let's look at a numerical example.

- 1. Let p = 7 and q = 13 be the two primes.
- 2. n = pq = 91 and $\phi = (p-1)(q-1) = 72$.
- 3. Choose *e*. Let's look among the primes.
 - Try e = 2. gcd(2, 72) = 2 (does not work)
 - Try e = 3. gcd(3, 72) = 3 (does not work)
 - Try e = 5. gcd(5, 72) = 1 (it works)

```
We choose e = 5.
```

4. Let's find d. We want to find d such that

$$ed \equiv 1 \pmod{\phi}$$

which is equivalent to find d such that

$$ed + \phi k = 1$$

for some integer k. Recall that $gcd(e, \phi) = 1$. We can use the Extended Euclid's Algorithm to find integers x and y such that

$$ex + \phi y = \gcd(e, \phi).$$

If e = 5 and $\phi = 72$, we find x = 29 and y = -2. Indeed, $5(29) + 72(-2) = \gcd(5, 72) = 1$. Then,

$$d = 29.$$

In general, we use $d = x \mod \phi$.

5. The encryption function is

$$E(M) = M^e \mod n = M^5 \mod 91.$$

The decryption function is

 $D(M) = M^d \mod n = M^{29} \mod 91.$

6. Suppose the message is M = 10.

$$E(M) = E(10) = 10^{\circ} \mod 91 = 82$$

$$D(E(M)) = D(82) = 82^{29} \mod{91} = 10$$

 Let's see how to compute efficiently 82²⁹ mod 91 using the square-and-multiply algorithm.

$$(82)^{1} \equiv 82 \pmod{91}$$
$$(82)^{2} \equiv 81 \pmod{91}$$
$$(82)^{4} \equiv (81)^{2} \equiv 9 \pmod{91}$$
$$(82)^{8} \equiv (9)^{2} \equiv 81 \pmod{91}$$
$$(82)^{16} \equiv (81)^{2} \equiv 9 \pmod{91}$$

Since 29 = 16 + 8 + 4 + 1 (in binary 29 is 11101), we deduce that

$$82^{29} \equiv (82)^{16} (82)^8 (82)^4 (82)^1 \pmod{91}$$

$$\equiv (9)(81)(9)(82) \pmod{91}$$

$$\equiv 10 \pmod{91}$$

We conclude that $82^{29} \mod 91 = 10$.

Typeset with $I\!AT_{\!E\!}\!X$ on June 11, 2007.