Breaking RSA

The public side of RSA consists of an encrypting exponent, e, and a modulus, m. The ciphertext, C, is found from the message by the formula

$$C = M^e \mod m$$

It is decrypted by a secret exponent d, where

$$ed = 1 \mod \phi(m)$$

Then

$$M = C^d \mod m$$

If we can manage to factor m, then computing $\phi(m)$ and d becomes routine.

The security of RSA depends on the fact that it is difficult to factor large numbers. When RSA was introduced in 1977, it was recommended that p and q be on the order of 80 digits each. By 1987 it was recommended that they be 200 digits each. Presently, 400 digit numbers should be used!

How can we factor m?

Check the primes between 2 and $\sqrt{m}$ to see if any divide m

For small m, this is the easiest and most efficient way of factoring an integer. On average it will take about $\sqrt{m}/2$ calculations to factor m.

Unfortunately, this becomes very inefficient for large m. Is there a better way?

Quadratic Sieve Factoring Algorithm

1. Pick random $a \in \{1, 2, \ldots, (m-1)/2\}$
2. If $gcd(a, m) > 1$ then DONE!
3. Otherwise compute $a^2 \bmod m$ and compare to other squares already computed. If there is another number $b \neq a$ such that
$$a^2 \equiv b^2 \mod m$$
then
$$(a+b)(a-b) = a^2 - b^2 \equiv 0 \mod m$$
This means that
$$(a+b)(a-b) = km$$
for some k. Since both $a+b$ and $a-b$ are less than m, m cannot divide either one. Therefore
$$m = gcd(m, a+b) \times gcd(m, a-b)$$

Quadratic Sieve

Example: $m = 91$

$$\begin{array}{c|ccccccc} a & 19 & 1 & 23 & 18 & 2 & 24 & 16 \\ \hline a^2 & 88 & 1 & 74 & 51 & 4 & 30 & 74 \end{array}$$

$$\begin{aligned} 91 &= gcd(91, 23+16) \times gcd(91, 23-16) \\ &= gcd(91, 39) \times gcd(91, 7) \\ &= 13 \times 7 \end{aligned}$$

Analysis of Quadratic Sieve

Claim: If $m = pq$ where $p, q > 1$, then for all $a \in \{1, 2, \ldots, (m-1)/2\}$ such that $gcd(a, m) = 1$, there is an integer $b \in \{1, 2, \ldots, (m-1)/2\}$ such that $b \neq a$ and $b^2 \equiv a^2 \bmod m$.

Example: $m = 21$

a	$gcd(a, m)$	$a^2 \bmod m$	b
1	1	1	8
2	1	4	5
3	3	9	
4	1	16	10
5	1	4	2
6	3	15	
7	7	7	
8	1	1	1
9	3	18	
10	1	16	4

Remark: Exactly 1/2 of the $\phi(m)$ integers that are relatively prime to m are between 1 and $(m-1)/2$ since

$$\gcd(a, m) = \gcd(m - a, m).$$

$$P(k) = \begin{array}{l}\text{Probability that a subset of } \{1, 2, \ldots, (m-1)/2\} \\ \text{of size } k \text{ that there is one number, } a\text{, that has} \\ \gcd(a, m) > 1 \text{ or there are two integers } a \neq b \\ \text{such that } a^2 \equiv b^2 \bmod m.\end{array}$$

$$= 1 - \begin{array}{l}\text{Probability that a subset of size } k \text{ such that} \\ \text{for all } a\text{, } \gcd(a, m) = 1 \text{ and for all } a, b\ a^2 \not\equiv b^2 \\ \bmod m.\end{array}$$

$$= 1 - \left(\frac{\frac{\phi(m)}{2}}{\frac{m-1}{2}} \cdot \frac{\frac{\phi(m)}{2} - 2}{\frac{m-1}{2} - 1} \cdot \frac{\frac{\phi(m)}{2} - 4}{\frac{m-1}{2} - 2} \cdots \frac{\frac{\phi(m)}{2} - 2k + 2}{\frac{m-1}{2} - k + 1} \right)$$

Example: $m = 6731$

$P(1) = .026 \qquad P(10) = .24 \qquad P(45) = .79 \qquad P(90) = .98$