Why of RSA:

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

(as long as a & m have no common factors)

so $a^{k\phi(m)} \equiv 1 \pmod{m}$

if $e \cdot d \equiv 1 \pmod{\phi(m)}$

then $e \cdot d - 1 = k\phi(m)$ for some k

$e \cdot d = 1 + k\phi(m)$ for some k

$M^e \equiv C \pmod{m}$

to decrypt:

$$\begin{aligned} C^d \equiv (M^e)^d \equiv M^{e \cdot d} &\pmod{m} \\ \equiv M^{k \cdot \phi(m) + 1} &\pmod{m} \\ \equiv M^{k \cdot \phi(m)} \cdot M^1 &\pmod{m} \\ \equiv 1 \cdot M^1 &\pmod{m} \\ \equiv M \end{aligned}$$

to compute d given e & $\phi(m)$

$d \cdot e + k \cdot \phi(m) = 1$

$e = 323$ $\quad \phi(m) = (1873-1)(131-1)$

$= 243360$

$(-55 - 753 \cdot 126) \cdot 323 + \cdots$

$= -55 \cdot 323 + 126(243360 - 753 \cdot 323 -$

$243360 = 753 \cdot 323 + 141$

$323 = 2 \cdot 141 + 41$

$141 = 3 \cdot 41 + 18$

$41 = 2 \cdot 18 + 5$

$18 = 3 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$= 16 \cdot 141 - 55(323 - 2 \cdot 141) = -55 \cdot 323 + 126 \cdot 141$

$= 16(141 - 3 \cdot 41) - 7 \cdot 41 = 16 \cdot 141 - 55 \cdot 41$

$= 2 \cdot 18 - 7(41 - 2 \cdot 18) = 16 \cdot 18 - 7 \cdot 41$

$= 2(18 - 3 \cdot 5) - 5 = 2 \cdot 18 - 7 \cdot 5$

$= 3 - (5 - 3) = 2 \cdot 3 - 5$

$1 = 3 - 2$

$e = -55 - 753 \cdot 126 = -94933 \equiv 148427 \pmod{\phi(m)}$

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

$m = 12 = 3 \cdot 4 = 3 \cdot 2^2$ $\quad \phi(m) = (3-1)(2^2-2) = 4$

$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ $\quad \phi(m) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots (p_k^{a_k} - p_k^{a_k-1})$

$\{1, 5, 7, 11\}$ theorem says $1^4 \equiv 5^4 \equiv 7^4 \equiv 11^4 \equiv 1 \pmod{m}$

$\downarrow \times 5 \pmod{12}$

$\{5, 1, 11, 7\}$

$(\mod m)$

$1 \cdot 5 \cdot 7 \cdot 11 \equiv 5 \cdot 1 \cdot 11 \cdot 7 \equiv (5 \cdot 1)(5 \cdot 5)(5 \cdot 7)(5 \cdot 11)$

$1 \equiv 5 \cdot 5 \cdot 5 \cdot 5 \pmod{12}$

$\{x_1, x_2, \ldots, x_{\phi(m)}\}$

$\downarrow$ a rel prime to m

$\{ax_1, ax_2, \ldots, ax_{\phi(m)}\}$

$x_1 x_2 \cdots x_{\phi(m)} \equiv ax_1 ax_2 \cdots ax_{\phi(m)} \pmod{m}$

$1 \equiv a^{\phi(m)} \pmod{m}$

permutation.

Computation elements needed to implement RSA

In order for RSA to be a useful system to implement, it must be possible to do the following types of calculations relatively quickly for very large integers. The complexity of these operations should grow no faster than $O((\text{number of digits})^d)$ in order for this system to be practical.

- compute $\phi(n)$ given $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ ✓ $\phi(n) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots (p_k^{a_k} - p_k^{a_k-1})$
- calculate a^b modulo n. ✓
- determine the inverse of an integer a modulo n. ✓
- find very large primes

The security of the RSA system relies on the fact that given an integer n which is the product of two large primes, it is computationally difficult to factor n. Therefore if we are to play the role of the opponent we would like an algorithm which also runs relatively quickly which can:

- factor very large integers

Primality Testing

The Jacobi symbol allows us to test for primality of n without carrying out its factorization.

if n is prime then $J(a,n) = \left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \pmod{n}$

If n is prime then

$$J(a,n) = a^{(n-1)/2} \mod n$$

Thus if this identity fails to hold for any value of a in $[1, n-1]$ we can certainly conclude that n is not a prime!

Theorem 5 *If n is not a prime then for more than one half the integers in $\{1, \ldots, n-1\}$ one of the following two tests will fail*

$$J(a,n) = a^{(n-1)/2} \qquad \gcd(a,n) = 1$$

To select a prime at random in a given range, we proceed as follows.

1. We first pick an (odd) integer n at random in the given range.

2. We next pick at random a certain (previously agreed upon) number k of integers $a_1, a_2, \ldots, a_k$ in the interval $\{1, \ldots, n-1\}$.

3. For each number, check that

$$gcd(a_i, n) = 1 \quad \text{and} \quad J(a_i, n) = a^{(n-1)/2} \mod n$$

If n happened to be prime then it will pass all of these tests. On the other hand, if n is not a prime, it will pass all of these tests with probability less than $(1/2)^k$.

Legendre Symbol

For a prime p

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \in QR[p] \\ -1 & \text{if } a \notin QR[p] \\ 0 & \text{if } gcd(a,p) > 1 \end{cases}$$

Then for a relatively prime to p, we have

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$$

Hence

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$

Theorem 4 (Quadratic Reciprocity) *For any two primes p and q we have*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

Jacobi Symbol

We start with the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \in QR[p] \\ -1 & \text{if } a \notin QR[p] \end{cases}$$

and for

$$n = p_1 p_2 \cdots p_k$$

we set

$$J(a,n) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$$

$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ $J(2,n) = (-1)^{(n^2-1)/8}$

However, for n odd, we have

$$J(a,n) = \begin{cases} 1 & \text{if } a = 1 \\ J(a/2,n)(-1)^{(n^2-1)/8} & \text{if } a \text{ is even} \\ J(n \mod a, a)(-1)^{(n-1)(a-1)/4} & \text{if } a > 1 \text{ and odd} \end{cases}$$

$J(a,n) \cdot J(n,a)$

a square number mod p

Quadratic Residues

Theorem 1 *For a prime p the equation*

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0 \pmod{p}$$

has at most n solutions.

Note that an equation may have no solution at all

$$x^2 = 2 \mod 5$$

$$1^1 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 4,\ 4^2 \equiv 1$$

Definition: We say that a is a *quadratic residue* mod p if

$$x^2 - a = 0 \mod p$$

has a solution x.

Quadratic Residues

Denote the set of quadratic residues by the symbol

$$QR[p] = \left\{ x^2 \bmod p \mid x \in \{1, 2, \ldots p-1\} \right\}.$$

Example

1. $p = 11$

x	1	2	3	4	5	6	7	8	9	10
x^2	1	4	9	5	3	3	5	9	4	1

$$QR[11] = \{1, 4, 9, 5, 3\}.$$

2. $p = 13$

x	1	2	3	4	5	6	7	8	9	10	11	12
x^2	1	4	9	3	12	10	10	12	3	9	4	1

$$QR[13] = \{1, 4, 9, 3, 12, 10\}.$$