How RSA Works with Maple

RSA Procedure:

1. Pick two primes p, q
2. Set n = p*q and m = (p –1)*(q – 1)
3. Pick a such that 1 < a < p – 1 and gcd (m, a) = 1
4. Find b such that a*b is congruent to 1 (mod m).
5. Publish (a, n) as the public key. Retain b as the private key.

Encoding Message M: send C = M^a (mod n)

Decoding Message C: compute M = C^b (mod n)

Note: In the text, there is a procedure to determine b that involves the parameter t. This does not work for large values of a and m. The Euclidean Algorithm replaces this procedure.

Note: In step 4, we use the power of Maple (via the function "inverse of a mod m", not the fraction 1/a) to calculate b directly with the line:

b:= 1/a mod m;

This gives b immediately.

Note: The RSA encryption works because:

$$
\begin{aligned}
C^b (\bmod n) &= \left(M^a (\bmod n)\right)^b (\bmod n) \quad [\textit{apply Law of Mod Mult}] \\
&= \left(M^a\right)^b (\bmod n) = \left(M^{ab}\right)(\bmod n) \\
&= \left(M^{1+t(p-1)(q-1)}\right)(\bmod n) \qquad [\textit{ for some } t] \\
&= (M)\left(M^{t(p-1)(q-1)}\right)(\bmod n) \qquad [\textit{apply Euler}; n = pq] \\
&= M (\bmod n) = M \qquad [\textit{because } M < n]
\end{aligned}
$$