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:

\[ C^b (\mod n) = (M^a (\mod n))^b (\mod n) \]
\[ = (M^a)^b (\mod n) = (M^{ab})(\mod n) \]
\[ = (M^{(p-1)(q-1)}) (\mod n) \]
\[ = (M)(M^{(p-1)(q-1)}(\mod n)) \]
\[ = M (\mod n) = M \]

[apply Law of Mod Mult]
[for some t]
[apply Euler; n = pq]
[because M < n]