Modular Exponentiation

This is a method for computing $a^b \mod n$ without knowing $\phi(n)$. (See also p. 125 in Erickson/Vazzana). As an example, we compute

$$2^{1234} \mod 789$$

First we use successive squaring:

$$2^2 \equiv 4 \mod 789$$

$$2^4 \equiv 16 \mod 789$$

$$2^8 = (2^4)^2 \equiv 16^2 \equiv 256 \mod 789$$

$$2^{16} \equiv 256^2 \equiv 49 \mod 789$$

$$2^{32} \equiv 49^2 \equiv 34 \mod 789$$

$$2^{64} \equiv 34^2 \equiv 367 \mod 789$$

$$2^{128} \equiv 367^2 \equiv 559 \mod 789$$

$$2^{256} \equiv 559^2 \equiv 37 \mod 789$$

$$2^{512} \equiv 37^2 \equiv 580 \mod 789$$

$$2^{1024} \equiv 580^2 \equiv 286 \mod 789$$

Since $1234 = 1024 + 128 + 64 + 16 + 2$ we get

$$2^{1234} = 2^{1024} \cdot 2^{128} \cdot 2^{64} \cdot 2^{16} \cdot 2^2 = 286 \cdot 559 \cdot 367 \cdot 49 \cdot 4 \equiv 481 \mod 789$$