The standard way to generate big prime numbers is to take a preselected random number of the desired length, apply a [Fermat test](http://en.wikipedia.org/wiki/Fermat_primality_test) (best with the base 22 as it can be optimized for speed) and then to apply a certain number of [Miller-Rabin tests](http://en.wikipedia.org/wiki/Miller-Rabin_primality_test) (depending on the length and the allowed error rate like 2−1002−100) to get a number which is very probably a prime number.

The preselection is done either by test divisions by small prime numbers (up to few hundreds) or by [sieving](http://en.wikipedia.org/wiki/Sieve_of_Eratosthenes) out primes up to 10,000 - 1,000,000 considering many prime candidates of the form b+2ib+2i (bb big, ii up to few thousands).

The deterministic prime number test by [AKS](http://en.wikipedia.org/wiki/AKS_primality_test) is to my knowledge not yet used as it is slower and as the likeliness that an calculation error caused by the hardware is higher than 2−1002−100.

Most smart cards offer a coprocessor for modular arithmetic with moduli from 1024 up to few thousand bits. The manufacturers often provide also libraries for RSA and RSA key generation using the coprocessor.