

METHOD AND SYSTEM FOR DERIVING DETERMINISTIC PRIME NUMBER

Abstract

This invention relates a system generating a prime number comprising a pseudorandom number generator (PRNG) module and a prime number generator (PNG) module. The PRNG module is configured to: initialise the pseudorandom number generator (PRNG) module; receive a request from the PNG module, the request containing a bit length of the pseudorandom number required; generate the required bit length of pseudorandom number; transmit a response containing the generated bit length of pseudorandom numbers to the PNG module. The PNG module is configured to: transmit the request containing the bit length of the pseudorandom numbers required; receive the response from the PRNG module; assign the pseudorandom numbers in the response to form raw data PPP ; set a least significant bit (LSB) and most significant bit (MSB) of PPP as 1 to obtain a first big odd number denoted as PP ; and execute an algorithm to determine a first big prime number starting from odd number PP .

Figure 1 to accompany the abstract