**Generatore di numeri primi**

Guido Pegna

La conoscenza di numeri primi molto grandi è diventata decisiva per le attuali necessità di sicurezza delle transazioni attraverso la rete Web, specialmente di quelle commerciali e finanziarie, oltre che per le comunicazioni militari. Infatti tutti gli attuali sistemi di crittografia sicura codificano il messaggio in chiaro per mezzo di “chiavi” numeriche molto grandi. La sicurezza si basa sul fatto che se la chiave è ottenuta come prodotto di due numeri primi molto grandi, è estremamente difficile trovare quali siano i due numeri primi componenti. Occorre infatti un processo di scomposizione in fattori che se il numero è sufficientemente grande può richiedere anni di calcolo di un supercalcolatore, se non addirittura, proprio teoricamente tempi superiori all’età dell’Universo (15 miliardi di anni!).

La proposta è la seguente. E’ interessante creare un programma che esegua un algoritmo efficiente per la generazione della successione dei numeri primi.