

Informazioni sull'eseguibile relativo a Primi Grandi

L'eseguibile presenta due opzioni: la prima è dedicata a verificare se un numero è Primo o Composto, la seconda è preposta a generare Numeri Primi. L'algoritmo utilizzato è quello noto nel campo della teoria dei numeri come metodo di Rabin–Miller. Tale algoritmo è di tipo probabilistico, nel senso che il numero verificato o generato risulta primo con una probabilità che non lo sia piccola a piacere. Nel presente contesto ad esempio la probabilità che un numero grande dichiarato primo non lo sia, risulta più piccola di 0.000000000000001.

Il campo di applicazione dei numeri che si possono trattare va da numeri formati da almeno cinque cifre sino ad un massimo di 500 cifre. L'eseguibile può essere utile pertanto anche nel campo della crittografia moderna a chiave pubblica dove occorre avere disponibili dei numeri primi random costituiti almeno da 150 ÷ 160 cifre. Non si sono presi in considerazione numeri con meno di cinque cifre in quanto la loro verifica o generazione può ad esempio essere effettuato molto efficacemente con semplici diversi algoritmi (vedi ad esempio il crivello di Eratostene, l'algoritmo delle Divisioni Successive, l'algoritmo di Fermat, i metodi di Gauss, di Legendre, ecc.)

Per una spiegazione ed illustrazione più approfondita e dettagliata sulle prestazioni di questo eseguibile si rimanda il lettore al seguente articolo: "Come Generare Numeri Primi Grandi" che compare sul presente Sito nella sezione Articoli dei lavori dell'ing. Teodoro Cristiano.