

Informazioni sull'Eseguibile relativo a “ **Equazioni Diofantee lineari con applicazione al calcolo della chiave Privata in RSA**”

l'Eseguibile è dedicato alla risoluzione delle equazioni indeterminate del tipo $ax + by = c$, a trovare cioè valori interi per le incognite x e y che soddisfino l'equazione, dove i valori a , b , c sono degli interi qualsiasi sia positivi che negativi. L'eseguibile inoltre risulta in grado di calcolare e trovare Chiavi Private necessarie nella realizzazione dell'algoritmo crittografico RSA. Poiché però nel programma viene adoperata solo l'aritmetica a doppia precisione messa a disposizione dal software de linguaggio Qbasic, per avere risultati sempre esatti occorre che i parametri introdotti ed utilizzati non abbiano valori numerici grandi costituiti ciascuno al massimo da non più di 5 o 6 cifre.