

Informazioni sull'Eseguibile "Calcolo della chiave Privata nell'algoritmo Crittografico RSA"

L'Eseguibile è dedicato alla generazione della **Chiave Privata d** , vale a dire alla risoluzione dell'equazione diofantea $e \cdot d - \Phi \cdot y = 1$ dove e è un numero dispari od numero primo random e $\Phi = (p - 1) \cdot (q - 1)$ con p e q numeri primi random grandi.

Con il presente eseguibile si è in grado di effettuare operazioni aritmetiche su valori numerici anche elevati e quindi di poter calcolare e trovare **concreti** valori di Chiavi Private di impiego effettivo, poiché le operazioni di calcolo sono programmate per una loro utilizzazione in aritmetica a precisione multipla.

L'eseguibile presenta due opzioni:

Prima opzione: dedicata al calcolo della Chiave Privata d introducendo dall'esterno, e quindi da richiesta di INPUT, tre numeri primi anche relativamente grandi, costituiti da stringhe di tipo numerico, riguardanti i seguenti tre parametri: e numero dispari e preferibilmente primo random⁽¹⁾;

p numero primo random formato anche da 160 cifre e oltre

q numero primo random formato anche da 140 cifre e oltre

Se si vuole generare una Chiave Privata di effettivo utilizzo i numeri p e q devono essere tali per cui $n = p \cdot q$ risulti costituito da almeno 309 cifre decimali (digit) pari ad un numero di bit non inferiori a 1024 bit. Si sottolinea l'esigenza che i numeri p e q debbono essere effettivamente dei numeri primi. Si fa comunque presente che almeno per qualsiasi valore sia di p che di q inferiore a 10^{15} l'eseguibile è in grado di verificare se i numeri p e q sono effettivamente primi. Per valori di p e di q più grandi occorre invece assicurarsi preventivamente che essi siano effettivamente primi perché si abbia un Chiave Privata valida.

Seconda opzione: relativa ad un esempio di calcolo di chiave privata d con i valori dei tre parametri suddetti con i requisiti richiesti già inseriti nel programma come dati costituiti da stringhe numeriche e quindi immediatamente disponibili.

Si fa presente infine che per una più facile lettura dei risultati numerici trovati, essi vengono mostrati a gruppi formati ognuno da sette cifre decimali separati in successione fra loro da uno spazio.