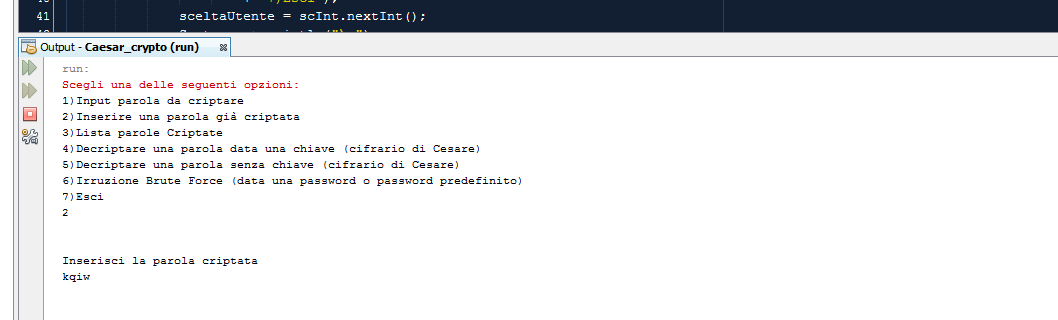
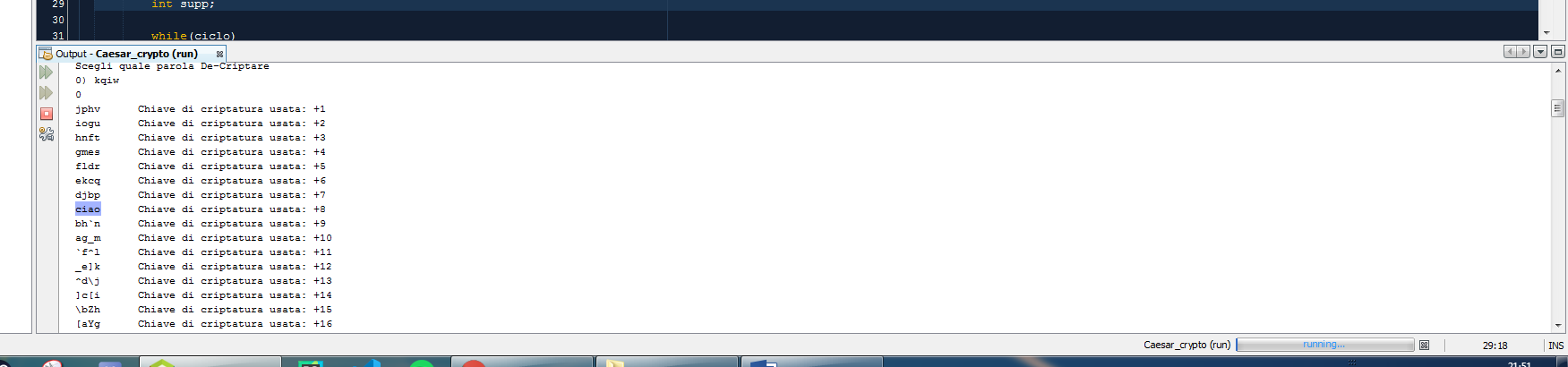
**Funzionamento Algoritmo di Brute Force**

Questo è un vecchio algoritmo che avevo fatto l’anno scorso come progetto scolastico, è un programma che comprende varie funzionalità di criptatura e decriptatura di messaggi, in questo specifico caso lo usiamo per decriptare forzatamente un messaggio precedentemente crifrato con il cifrario di Cesare (usando la chiave creata e scambiata dell’algoritmo precedente, Diffie Hellman).

L’algoritmo inizia mostrando il seguente menù con le seguenti opzioni, nel nostro caso dobbiamo immettere per prima nel programma la parola già cifrata in modo da immagazzinarla nel programma:



Poi dobbiamo scegliere l’opzione 5 (decifratura forzata) per poter ricavare una serie di parole usando una serie di chiavi:



E possiamo notare come in mezzo a quelle parole senza senso, compaia una parola in chiaro, in questo modo possiamo sapere che quella era la parola originaria.