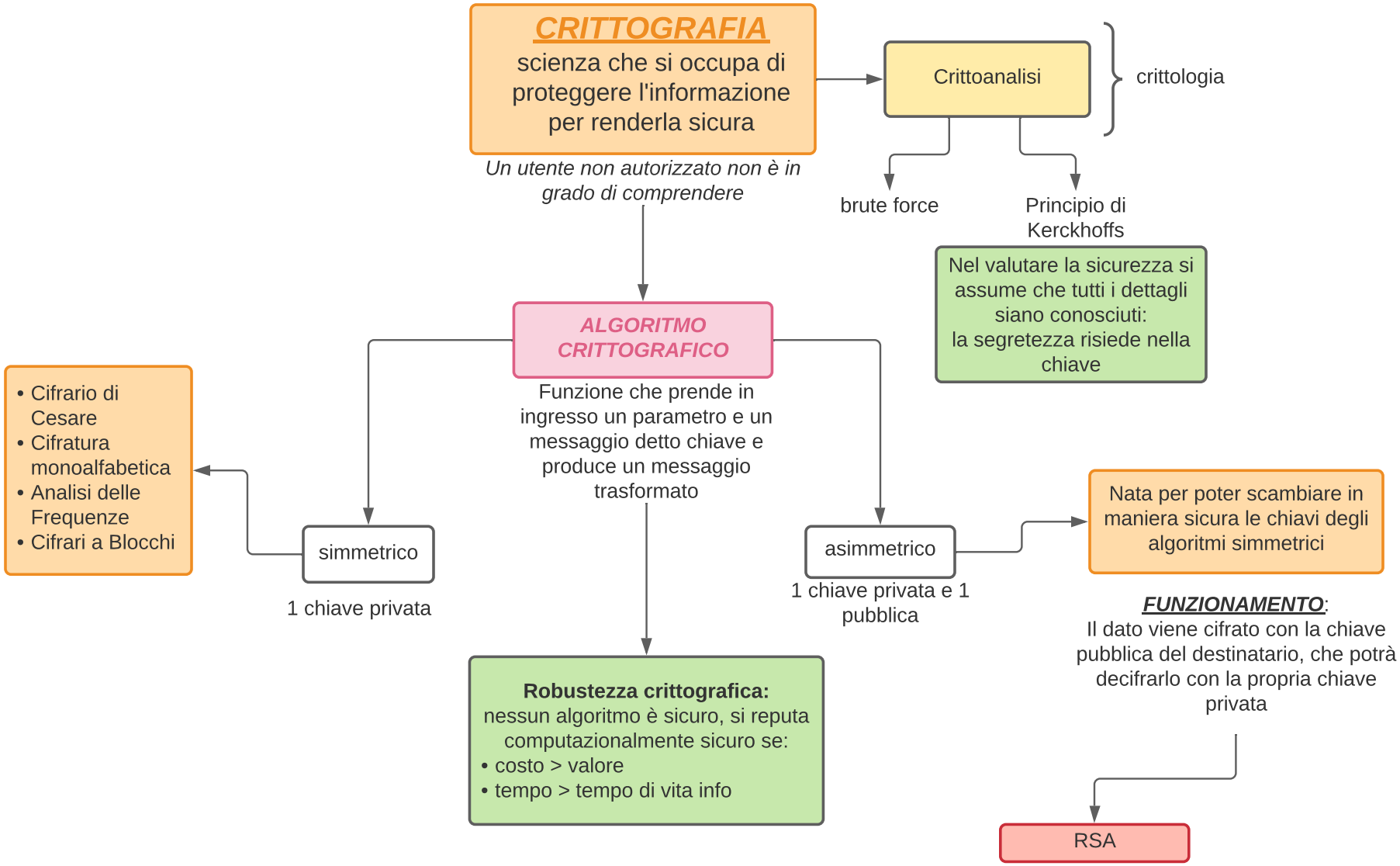

Il funzionamento del metodo RSA si può schematizzare con i seguenti punti:

1. si scelgono due numeri primi,*peq*;
2. si calcola il loro prodotto$N=p\times q$, chiamato*modulo*(datoche tutta l'aritmetica seguente è*modulo N*);
3. si sceglie poi un numeroe(chiamato*esponente pubblico*), più piccolo di$N$e primo rispetto a f (N) = ($p-1$)× ($q-1$), dove f è la funzione di Eulero;
4. si calcola il numero$d$(chiamato*esponente privato*) tale chee×d–> 1mod(($p-1$)× ($q-1$)).

La chiave pubblica è rappresentata dalla coppia di numeri (N,e), mentre la chiave privata è rappresentata da (N,d).