Durante la seconda prova d'esame potrà essere richiesto di dimostrare formalmente uno dei seguenti risultati, presentati a lezione e riportati sul libro di testo indicato.

1) Correttezza e/o complessità in bit dell'algoritmo di Euclide
2) Correttezza del protocollo RSA
3) Master theorem per le ricorrenze del tipo: $T(n)=aT(n/b)+O(n^d)$
4) Un grafo diretto ha un ciclo se e solo se la DFS eseguita su di esso rivela un back-edge
5) Correttezza della *proprietà di taglio* (*cut property*), da cui deriva la correttezza degli algoritmi di Kruskal e di Prim
6) Rango massimo degli elementi presenti in una struttura per insiemi disgiunti gestita con *union-by-rank*
7) Fattore di approssimazione per l'algoritmo greedy presentato come soluzione al problema del *set cover*