

Reti di calcolatori - ITPS - a.a. 08/09
Appello del 29/01/09 (durata: 2 ore)

1. Cos'è e a cosa serve un protocollo di broadcast (fornire un esempio).
2. Descrivere le differenze fra un sistema a chiave pubblica ed un sistema a chiave simmetrica.
3. Si suppone che N pacchetti arrivino contemporaneamente ad un collegamento nel quale non vi sono altri pacchetti in corso di trasmissione o in coda. Ciascun pacchetto è di lunghezza L e la frequenza di trasmissione è R . Calcolare il ritardo medio di accodamento per gli N pacchetti.
4. Quale dei problemi dei cifrari a blocchi viene risolto dalla tecnica chiamata Cipher Block Chaining (CBC)?
5. Confrontare ed evidenziare differenze tra algoritmi di instradamento a stato di collegamento e con vettore di distanza.
6. E' possibile per un'applicazione su UDP ottenere trasferimento dati affidabile? Se sì, come?
7. Supponiamo che due nodi inizino a trasmettere nello stesso istante un pacchetto di lunghezza L su un canale broadcast con tasso trasmissivo R . Indicando con t_{prop} il ritardo di propagazione fra i due nodi, dire se nel caso $t_{prop} < L/R$ ci sarà collisione e spiegare il perché.
8. Quali sono i vantaggi di uno schema di controllo di parità bidimensionale?
9. Descrivere brevemente i protocolli Go-Back-N (GBN) e a ripetizione selettiva (SR) ed evidenziare le differenze.
10. L'algoritmo RSA è
 1. un algoritmo di crittografia a chiave simmetrica
 2. un algoritmo di instradamento
 3. un algoritmo di crittografia a chiave pubblica