

**Corso di Laurea in Ingegneria Informatica
Anno Accademico 2015/2016**

Proff. Stefano Leonardi and Andrea Vitaletti, 15 Luglio 2016

75 minuti

Domanda 1. Si consideri un'applicazione telefonica su Internet con codifica PCM ed un ritardo di trasmissione medio di 100 msec.

1. Si progetti una codifica che permetta di recuperare un pacchetto perso ogni 4 pacchetti trasmessi.
2. Determinare il minimo ritardo di playout necessario per la trasmissione.
3. Determinare la perdita di banda introdotta dalla codifica.

Domanda 2. Si consideri il protocollo HTTP.

1. Il protocollo permette la possibilità di memorizzare lo stato della sessione?
2. Come è possibile permettere l'accesso dei client solo attraverso autenticazione?
3. Si illustri una modalità per tenere traccia delle pagine web visitate da un client.

Domanda 3. L'overlay network di una rete P2P è un albero binario con radice R. Il nodo A si trova al livello 3 del sottoalbero di sinistra (rispetto ad R), mentre il nodo B si trova al livello 2 del sottoalbero di destra (rispetto ad R). Supponiamo che A ricerchi un file F che si trova in B.

- 2.1 Quanti messaggi sono necessari per trovare F in un'architettura di tipo Gnutella? Se il TTL dei messaggi di ricerca fosse 3, F verrebbe trovato?
- 2.2 Quanti messaggi sono necessari per trovare F in un'architettura di tipo Napster? Se il TTL dei messaggi di ricerca fosse 3, F verrebbe trovato?

Domanda 4. Si consideri un Key Distribution Center (KDC)

- 1.1 Qual'è il vantaggio di usare una Key Distribution Center (KDC) rispetto ad avere una chiave per ogni coppia di utenti? Quantificare la risposta nel caso di N utenti.
- 1.2 Qual informazione deve essere condivisa tra il KDC e ciascun utente?
- 1.3 Come si fa a condividere una chiave di sessione usando un KDC?
- 1.4 Che differenza c'è tra una Key Distribution Center (KDC) ed una Certification Authority (CA)?

Acconsento alla pubblicazione dei risultati sul Web

Nome e Cognome in stampatello

Firma