Esame di **Progettazione di servizi web e reti di calcolatori (01NBE)**
Corso di Laurea in Ing. Gestionale
Prova scritta di teoria (17/7/2020)

> NOTA
> Le tracce delle soluzioni fornite in questo testo sono da considerarsi solo come un aiuto per comprendere i principali punti da toccare nel risolvere gli esercizi proposti ma non sono né esaustive né presentate in forma adeguata per l'elaborato da consegnarsi in sede d'esame.
> In particolare per molti esercizi le soluzione è volutamente schematica e ci si attende che il candidato spieghi adeguatamente i singoli punti, per dimostrare reale comprensione dell'argomento invece che semplice capacità mnemonica di ricordare i punti elencati nelle slide (o in queste tracce di soluzione).

Esercizio 1 ***(punti: 6)***

HTTP/1.1 usa per default connessioni persistenti. Spiegare di cosa si tratta e quali sono i vantaggi e svantaggi rispetto alle connessioni standard HTTP/1.0.

Traccia di una possibile risposta

In HTTP/1.1 le connessioni non sono più chiuse automaticamente dopo la risposta del server (come capitava in HTTP/1.0) ma quando il client segnala di voler terminare le comunicazioni (oppure quando la connessione resta inattiva per un tempo superiore al timeout).

Vantaggi: su un stessa connessione è possibile effettuare più richieste e ricevere più risposte, risparmiando in questo modo sul tempo di TCP setup (3-way handshake) e shutdown (4-way teardown) e conservando la window TCP.

Svantaggi: i client possono monopolizzare le risorse del server.

Esercizio 2 ***(punti: 6)***

In HTTP/1.1 è stata introdotta la codifica "chunked". Spiegare di cosa si tratta, come viene implementata in HTTP, quale problema risolve e quale problema potrebbe verificarsi in quei protocolli (come HTTP/1.0) che non ne dispongono.

Traccia di una possibile risposta

La codifica chunked serve a trasmettere una risposta la cui dimensione non è nota a priori e non è quindi possibile dichiararne la dimensione tramite l'header Content-length.

In HTTP viene implementata dichiarando nell'header "Transfer-encoding: chunked" e poi trasmettendo nel body la risposta frammentata. Ogni frammento è preceduto dalla sua dimensione in byte, espressa in esadecimale.

Risolve il problema delle risposte generate dinamicamente (come quelle prodotte da uno script PHP).

In HTTP/1.0 se una risposta dinamica veniva troncata a causa di un problema di rete, il client non poteva accorgersene perché non sapeva quanti dati doveva ricevere e quindi poteva erroneamnete creder di aver ricevuto tutta la risposta.

Esercizio 3 ***(punti: 6)***

Dato un documento elettronico (ad esempio un semplice file di testo) spiegare con quale procedura è possibile calcolarne la firma digitale, indicando anche gli specifici algoritmi coinvolti e di quali elementi deve essere dotato il firmatario per poter apporre la firma.

Traccia di una possibile risposta

La firma digitale di un file è la cifratura asimmetrica (con la chiave privata del firmatario) di un opportuno digest del file. In formula:

firma = enc (K_pri, digest (file))

La cifratura potrebbe avvenire con algoritmo RSA.

Il digest potrebbe essere calcolato con l'algoritmo SHA-256.

Il firmatario deve essere dotato (A) di una coppia di chiavi privata-pubblica, (B) la chiave pubblica deve essere associata ad un certificato X.509 per garantire la corrispondenza tra identità del firmatario e chiave, (C) un sistema sicuro per la generazione della firma, che può essere una smart-card o un computer dotato di un opportuno software.

Esercizio 4 ***(punti: 6)***

Con riferimento alla posta elettronica Internet, spiegare che cosa sono gli MTA, MSA e MS.

Traccia di una possibile risposta

MTA (Mail Transfer Agent) = uno dei tanti server intermedi tra mittente e destinatario; ha il compito di trasferire il messaggio al prossimo MTA della catena.

MSA (Mail Submission Agent) = primo server della catena di trasmissione; riceve il messaggio direttamente dal mittente e lo inoltra al primo MTA della catena.

MS (Mail Store) = server che contiene le caselle di posta degli utentei; ad esso si rivolge un utente per consultare la posta in arruivo.

Esercizio 5 ***(punti: 6)***

Un server web è ospitato su un nodo con scheda di rete a 1 Gbps collegata al backbone di campus che opera alla stessa velocità. Il campus usa degli switch aventi tutte le porte (inclusa quella verso il backbone) da 100 Mbps. A questi switch sono collegati nel laboratorio A 20 studenti e nel laboratorio B 10 studenti, ciascuno tramite un PC con scheda di rete a 10 Mbps.

Nel laboratorio A 15 studenti devono scaricare dal server un file da 50 MB e 5 studenti un file da 100 MB mentre nel laboratorio B gli studenti scaricano tutti un file da 50 MB.

Calcolare il tempo minimo dopo il quale tutti gli studenti hanno scaricato il file richiesto.

Traccia di una possibile risposta

Il server vorrebbe dividere in modo equo la banda tra tutti gli studenti, ossia

$1\,\text{Gbps}/30 = 33\,\text{Mbps}$ *per studente*

*ma questo valore eccede sia la capacità del singolo PC (*10 Mbps*) sia la capacità aggregata del singolo switch (*100 Mbps*). Quindi gli studenti si divideranno equamente la banda dello switch.*

Inizialmente nel laboratorio A $100\,\text{Mbps}/20 = 5\,\text{Mbps}$ *per studente. Quindi i 15 studenti che devono scaricare* 50 MB *finiranno dopo un tempo pari a:*

$T_{A,15} = 50\,\text{MB}/5\,\text{Mbps} = 80\,\text{s}$

A questo punto restano a lavorare solo i 5 studenti che devono scaricare altri 50 MB *(per arrivare al loro totale di* 100 MB*) ed andranno più veloci visto che ci sono meno utenti, ovvero a* 10 Mbps *e quindi impiegheranno un tempo aggiuntivo pari a:*

$T_{A,5} = 50\,\text{MB}/10\,\text{Mbps} = 40\,\text{s}$

Il tempo totale del laboratorio A sarà:

$T_A = T_{A,15} + T_{A,5} = 120\,\text{s}$

Invece nel laboratorio B $100\,\text{Mbps}/10 = 10\,\text{Mbps}$ *per studente. Quindi avranno terminato il loro lavoro dopo un tempo pari a:*

50 MB / 10 Mbps = 40 s

Visto che i due laboratori lavorano simultaneamente, il tempo totale sarà il massimo dei due, ossia 120 s.

Esercizio 6 ***(punti: 3)***

Assumendo di aver eseguito il seguente comando:

```
nslookup -q=MX piemonte.net
```

indicare quali possibili risposte (positive o negative) posso ottenere e che cosa ciascuna di esse indica.

Traccia di una possibile risposta

Una risposta positiva contiene l'elenco degli incoming mail server, ossia quei server che accettano di ricevere posta per utenti del dominio piemonte.net; questo elenco è ordinato per priorità (prima si devono contattare i server che hanno un numero inferiore).

Una risposta negativa indica invece che piemonte.net non è un dominio di posta ma uno specifico di rete e bisogna quindi trovarne l'indirizzo IP per contattarlo (ad esempio tramite una query nslookup -q=A piemonte.net+).