Esame di **Progettazione di servizi web e reti di calcolatori (01NBE)**
Corso di Laurea in Ing. Gestionale
Prova scritta di teoria (22/1/2021)

> 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)***

Se un utente A crea un messaggio cifrandolo con la chiave pubblica di un altro utente B, chi e come potrà leggere il contenuto del messaggio cifrato? quale funzionalità di sicurezza e stata ottenuta?

Se invece l'utente A crea un messaggio cifrandolo con la propria chiave privata, chi e come potrà leggere il contenuto del messaggio cifrato? quale funzionalità di sicurezza è stata ottenuta?

Traccia di una possibile risposta

Nel primo caso, solo l'utente B (che detiene la chiave privata corrispondente alla chiave pubblica usata per la cifratura) potrà leggere il contenuto del messaggio cifrato decifrandolo con la sua chiave privata; si è quindi ottenuta la proprietà di riservatezza (senza aver condiviso chiavi segrete).

Nel secondo caso, qualunque persone potrà leggere il contenuto del messaggio decifrandola con la chiave pubblica di A (che è appunto pubblica); in questo modo si è ottenuta l'autenticazione del mittente perché solo lui detiene la chiave privata usata per cifrare il messaggio.

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

Descrivere lo schema di una possibile architettura web 3-tier, illustrarne i componenti e discuterne vantaggi e svantaggi.

Traccia di una possibile risposta

Le architetture web sono composte da un'interfaccia utente, divisa tra parte client (implementata dal browser) e parte server (implementata da un server HTTP), la logica applicativa ed i dati.

In un'architettura web 3-tier, il primo livello è sempre il browser, il secondo livello è il server HTTP che può ospitare anche la logica applicativa (delegando al terzo livello la gestione dei dati)

Per lo schema si vedano le slide intitolate "3-tier: modello web (caso I)" e "3-tier: modello web (caso II)".

Vantaggi e svantaggi di ciascuna soluzione sono relativi al carico sui vari livelli.

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

Tre utenti, A, B e C, sono collegati ad Internet tramite linee ADSL, tutte da 20 Mbps in download ma con diversa velocità di upload, rispettivamente 5, 10 e 20 Mbps per A, B e C.

L'utente A deve ricevere da B e da C tramite HTTP due diversi file, ciascuno da 100 MB.

Sapendo che tutti i trasferimenti avvengono simultaneamente ed assumendo la velocità di Internet infinita, calcolare dopo quanto tempo termina ciascuno dei due trasferimenti.

Traccia di una possibile risposta

Siamo nella situazione in cui due nodi, B e C, inviano dati ad uno stesso terzo nodo, A. La velocità in download tra Internet ed A è di 20 Mbps *mentre la velocità in upload da B ad Internet è di* 10 Mbps *e da C ad Internet è di* 20 Mbps*.*

Siccome i due trasferimenti avvengono simultaneamente, c'è un collo di bottiglia sul nodo A e quindi - essendoci due trasferimenti simultanei - la banda disponibile verrà divisa a metà tra i due trasferimenti, ossia 10 Mbps *ciascuno.*

Ne consegue che il trasferimento da B ad A avverrà alla velocità di 10 Mbps*, come pure quello da C ad A. Quindi i due tempi saranno identici e pari a:*

$$t = 100\,\text{MB} \times 8/10\,\text{Mbps} = 800\,\text{Mb}/10\,\text{Mbps} = 80\,\text{s}$$

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

Con riferimento a HTTP/1.1, spiegare che cosa è il *pipelining*, quali benefici apporta e quali problemi può generare.

Traccia di una possibile risposta

Normalmente un client che invia una richiesta HTTP ad un server deve aspettare la relativa risposta prima di effettuare una nuova richiesta. Col pipelining, un client può inviare più richieste senza aspettare la risposta poer ciascuna di esse. Le risposte verranno inviate dal server nell'ordine corrispondente a quello delle richieste.

Il maggior vantaggio consiste nella velocità di risposta perché le richieste sono accorpate tutte insieme in un numero di segmenti TCP inferiore e non occorre attendere la risposta per ciascun richiesta.

Il principale svantaggio è che in caso di errore il client potrebbe dover rimandare tutte le richieste, anche quelle che hanno già ricevuto risposta.

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

Spiegare il funzionamento dei campi SYN, ACK, SequenceNumber e AcknowledgmentNumber in un segmento TCP, indicandone la correlazione e facendone un esempio con valori numerici concreti.

Traccia di una possibile risposta*SYN e ACK sono flag mentre SN ed AN sono campi numerici, tutto all'interno dell'header di un segmento TCP.*

Se SYN=1 si tratta del primo segmento di una trasmissione ed il SN indica la posizione iniziale nello stream di dati da cui partire per inserire i dati trasmessi nei segmenti successivi. Ad esempio, SYN=1 e SN=30 indica che i dati trasmessi nei segmenti successivi dovranno essere inseriti a partire dalla posizione 31.

Se SYN=0 si tratta di un segmento dati ed il SN indica la posizione nello stream di dati da cui partire ad inserire i dati trasmessi nel segmento stesso. Ad esempio, SYN=0 e SN=64, indica che i dati contenuti nel segmento devono occupare le posizioni 64, 65, 66, ...

Se ACK=1 allora AN conterrà la posizione dell'ultimo dato ricevuto correttamente. Ad esempio, ACK=1 e AN=70 indica che tutti i dati sino alla posizione 70 sono stati ricevuti correttamente ed il prossimo che ci si aspetta di ricevere è quello della posizione 71.

Se ACK=0, il segmento non indica nessuna conferma per dati già ricevuti ed il campo AN non è significativo