Prova scritta del modulo di Impianti Informatici a.a. 2016/2017
Corso di Laurea in Ingegneria Informatica (ord. 270)
(voto max di ogni quesito = 6 punti; la prova si intende superata con voto >= 18)

1) Descrivere sinteticamente le quattro principali classi di sistemi di elaborazione individuate dalla tassonomia di Flynn. Descrivere quindi la suddivisione in sottoclassi della classe MIMD e descrivere in dettaglio un aspetto specifico che caratterizza il funzionamento dei sistemi appartenenti ad una di tali sottoclassi, a scelta dello studente.

2) Anche facendo riferimento all'architettura astratta di un impianto informatico, descrivere a livello generale i diversi livelli di garanzia sull'effettiva trasmissione che possono essere forniti da un meccanismo di scambio di messaggi, discutendone vantaggi e svantaggi. Fare quindi un esempio concreto di un sistema, protocollo o applicazione che utilizza lo scambio di messaggi, descrivendone brevemente il funzionamento e commentando il livello di garanzia adottato in tale contesto.

3) Un amico vi dice "In ambito automobilistico le vetture con le maggiori prestazioni, come quelle da corsa, non sono le più affidabili ed hanno problemi tecnici piuttosto frequenti rispetto all'auto che io uso tutti i giorni. Si può fare un discorso del genere anche per i calcolatori ed i sistemi informatici in generale? Mi verrebbe naturale pensare che i calcolatori ad altissime prestazioni possano essere più delicati e più soggetti a guasti rispetto al mio PC di casa, perché i loro componenti sono più stressati. E' proprio così? Altrimenti mi sapresti dire che tecniche si possono usare per aumentare l'affidabilità di questi sistemi? Magari però i sistemi informatici sono più deterministici delle automobili ed esistono tecniche per prevedere i guasti e anticiparli in modo che in pratica non si verifichino mai. Se fosse così, avremmo dei sistemi che funzionano praticamente in eterno, non come le automobili. Tu che ne dici?" Cosa gli rispondereste?

4) Discutere a livello generale la differenza tra protocolli stateful e stateless nell'ambito delle architetture client-server discutendone vantaggi e svantaggi. Fare quindi un esempio concreto di protocollo stateful ed uno di protocollo stateless, descrivendone il funzionamento, evidenziandone le caratteristiche specifiche legate alla presenza o assenza di stato, e commentando le motivazioni che hanno portato all'adozione dell'approccio stateful o stateless nei due casi.

5) Definire in termini generali il problema dell'elezione del coordinatore, spiegare quali meccanismi possono essere usati per svolgere tale elezione e fare esempi concreti di situazioni nelle quali l'elezione si rende necessaria.

La sesta domanda è sul retro del foglio.

6) Il seguente testo, tratto dal sito di un'azienda che fornisce soluzioni di sicurezza, descrive i vantaggi di una soluzione innovativa per la protezione di web server contro attacchi DDoS rispetto ad altre soluzioni disponibili sul mercato.

A good conventional defence against DDoS attacks usually involves blocking a wide range of IP addresses.
The main problem with this method, however, is that significant segments of the network components such as public Wi-Fi networks, business centers, neighbourhoods and even small towns could be set to offline mode to safeguard against further DDoS attacks.
A superior security company is usually regarded by the amount of the IP addresses it is able to detect and block during a potential attack.

Solution:
Only malicious automated queries are blocked.
Legitimate users from IP address of "intruder" do not end up being affected. Even during an active DDoS attack, basic business operations should function without any interruptions.
Ultimately, customers may continue using the service and the service provider will maintain its visitor frequency and database.

Si richiede di discutere e commentare il testo facendo preferibilmente riferimento alle seguenti domande (con libertà di aggiungere ulteriori considerazioni personali):

1) Cosa sono gli attacchi DDoS e perché per difendersi vengono bloccati numerosi indirizzi IP?

2) Perché questo metodo di difesa potrebbe escludere anche degli utenti legittimi e non solo gli attaccanti?

3) Cosa è ragionevole ipotizzare sul funzionamento della soluzione innovativa stante il fatto che riesce a distinguere le richieste legittime da quelle ostili a parità di indirizzo IP di provenienza?

4) Spiegare la differenza tra protocollo HTTP e protocollo HTTPS. Quindi, anche tenendo conto del punto 3, commentare a livello generale le possibili differenze tra tecniche di difesa per attacchi DDoS condotti usando HTTP e tecniche di difesa per attacchi DDoS condotti usando HTTPS.