Aplicacions i Serveis a Internet

durada 2h

Final - Juny 2020

1. Preguntes cert o fals. Justifiqueu la resposta. Les respostes incorrectes resten. Les respostes sense justificació compten la meitat. (26)

   a) El servei de noms de domini consisteix en generar una base de dades mundial on existeixen registres de diferents tipus on algun d'aquests registres tenen a veure amb l'adreça IP

   b) El DNS està estructurat golbalment en forma d'arbre binari

   c) Els servidors DNS locals sempre han d'estar a la xarxa LAN on ofereixen el servei

   d) Podem tenir servidors DNS autoritat que tinguin adreçament privat sempre i quan siguin accessibles per qualsevol dispositiu que estigui a Internet

   e) Els registres tipus A no poden tenir adreces de tipus privat

   f) El servei de noms de domini també fa la conversió entre adreça IP i nom de domini

   g) Els servidors de correu receptors poden fer servir alguns registres del servei de noms de domini per confirmar la autenticitat dels servidors de correus emissors

   h) Un servidor de correu que fa de smarthost verifica els servidors que el fan servir en funció dels dominis pel que fa de smarthost

   i) Un servidor de correu que envia els missatges a un smarthost es basa en el domini del destinatari del missatge de correu

   j) Un servidor de correu rep missatges des d'Internet d'aquell servidor de correu que estigui a la llista de dominis que accepta

   k) La tecnologia Asynchronous Javascript and XML serveix per a que un navegador web pugui fer peticions web a qualsevol servidor web

   l) Un script Javascript a part d'interactuar localment amb els recursos del navegador web on s'executa, també pot interactuar amb el servidor web des d'on s'ha descarregat aquest script i només amb ell.

   m) Entre una transacció HTTP i la següent no hi ha cap mena de relació. És a dir, una no depèn de l'altre

   n) Si no ha d'intervenir un tercer C, la signatura digital d'una transacció de A cap a B pot simplificar-se per una autentificació de A per part de B en aquesta transacció

   o) És possible servir més d'una web en una xarxa privada i que es pugui accedir a elles amb diferents noms de domini només obrint únicament el port 80 de l'encaminador NAT que és l'únic que té l'adreça pública.

   p) El certificat d'usuari d'algú qualsevol és fiable només si el rebo d'una Autoritat de Certificació

   q) Les autoritats de certificació s'encarreguen de generar el certificat digital i han de proporcionar-te la clau privada associada a aquest certificat

   r) Si una persona genera el parell de claus públic i privat, pot xifrar missatges per a ella mateixa i signar missatges per tothom

   s) El mecanisme que té el servidor ssh per autentificar un client consisteix en que el client proporciona al servidor la clau pública de manera que cada vegada que es connecti, el servidor pugui comprovar que és ell. En canvi el servidor no cal que generi cap parell de claus

   t) Un certificat digital és el resultat de xifrar el valor de la clau pública d'una identitat, fent servir la clau privada d'una altra entitat de la que coneixes de manera fiable el valor de la seva clau pública

   u) Quan unes claus caduquen, els documents signats amb aquestes claus també caduquen

   v) Si canviem la contrasenya de la clau privada, en realitat estem canviant la clau privada

w) Quan es compra un domini, el gestor al que li contractes demana al responsable del top level domain una entrada a la seva base de dades amb un registre NS del domini registrat cap a un servidor de DNS autoritatiu gestionat pel propi gestor

x) Quan acceptem les cookies d'un lloc web, aquest lloc podria accedir a la informació personal que tenim al nostre ordinador

y) El protocol HTTPS garanteix la confidencialitat de la informació entre client i servidor a més de garantir l'autenticació de servidor però no de client

z) Les aplicacions P2P obliguen a obrir els ports dels encaminadors NAT que tenim a casa

2. Respon sí o no i justifica si els següents mecanismes serveixen per autentificar múltiples vegades (evitar atac de gravació) a un usuari A davant d'un usuari B. Considereu que si no es diu el contrari, la comunicació no està xifrada. Quan es parla de contrasenya, tant A com B la coneixen. (8)

a) Usuari B envia un missatge aleatori m a A. A retorna a B el missatge H(m) com a prova de la seva identitat, on H(m) és el resultat d'aplicar una funció de hash coneguda.

b) Usuari B envia un missatge aleatori m1 a A. A retorna a B el missatge H(m1|m2) on m2 és un missatge aleatori generat per A i m1|m2 és la concatenació dels dos missatges. H() és una funció de hash coneguda.

c) Usuari B envia un missatge aleatori m a A. A retorna a B el missatge K(m) que és el resultat d'aplicar una transformació a m on aquesta funció K() de transformació només és coneguda per A i B.

d) Usuari B envia un missatge aleatori m a A. A retorna a B el missatge H(m1|m2) on m2 és un missatge fixe conegut només per A i per B. H() és una funció de hash coneguda.

e) Usuari B espera la recepció d'un missatge c de A, on c és un la contrasenya associada a A.

f) Usuari B espera la recepció d'un missatge m de A, on m = KBp(c) és la contrasenya associada a A xifrada amb la clau pública de B.

g) Usuari B espera la recepció d'un missatge m de A, on m = K(c) és la contrasenya associada a A xifrada amb una clau només coneguda per A i B.

h) Usuari B envia un missatge aleatori m1 a A. A retorna a B el missatge KBp(m2) on m2 és un missatge aleatori generat per A. La concatenació K = m1|m2 és la clau de sessió d'un algoritme conegut de xifrat simètric. Usuari A envia K(c) a B, on c és la contrasenya associada a A i coneguda per B.

3. Considereu el següent algoritme: (6)

- Es busca dos nombres primers p, g on $p>g$. Aquests nombres s'intercanvien entre l'interlocutor I_A i el I_B.
- L'interlocutor I_A genera un nombre aleatori $a<p$ i calcula $A = g^a mod\, p$ que envia a I_B.
- L'interlocutor I_B genera un nombre aleatori $b<p$ i calcula $B = g^b mod\, p$ que envia a I_A.
- a i b són només coneguts per I_A i I_B respectivament.
- $I_A$calcula $K_A = B^a mod\, p$ i $I_B$calcula $K_B = A^b mod\, p$

a) Demostreu que $K = K_A = K_B$

b) Justifiqueu el perquè algú que observi l'intercanvi de missatges no pot aconseguir el valor de K

c) Calculeu el valor que surt de K tant per l'interlocutor I_A com $I_B$considerant els següents valors p=23, g=5, a=6, b=7.