Aplicacions i Serveis a Internet

durada 3h

Final - Juny 2016

1. Aplicant l'algoritme RSA, desxifreu el següent missatge: VOFUM. Teniu en compte que p=3, q=11 i e=7 (s'ha de trobar el valor correcte de d). (1)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
R	S	T	U	V	W	X	Y	Z	_	Ç	Ñ	*	#	@	+	
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	

2. Un amic vostre vol començar una aventura com empresari. Aquest amic és molt conscient de la importància que té donar una bona imatge respecte als recursos TIC, per aquest motiu us demana assessorament per muntar una web i unes bústies de correu. Com al començament està malament de diners, decideix utilitzar servidors gratuïts tant per les bústies de correu com per la web. Disposa del compte pepet1234@bustiagratis.com com de la web aprofita.webgratis.com/pepetlleig. En tot cas, el que està disposat a pagar és el domini pepet.cat. El gestor de domini, a més de poder definir qualsevol aspecte sobre el servei de noms, li permet definir qualsevol tipus de configuració sobre un servidor web i un servidor de correu del propi gestor, però no és possible allotjar cap tipus de dada. Aquest amic tampoc es pot permetre la instal·lació d'un servidor propi. Aquest amic us demana poder rebre correus dels comptes info@pepet.cat i comandes@pepet.cat i que la gent accedeixi a la seva web tant amb pepet.cat com www.pepet.cat. És possible satisfer les seves necessitats amb aquestes restriccions? Indiqueu si cal algun recurs extra més. Proposeu de quina manera s'haurien de configurar tant el servei de DNS, el servidor web i el servidor de correu del gestor. Recordeu que en el servei de DNS els principals registres que es poden definir són: NS, A, CNAME, MX. Recordeu que en el servei web algunes de les directives sobre les que s'ha treballar han sigut: VirtualHost, DocumentRoot, ServerName, Location, ProxyPass, ProxyPassReverse, Redirect, Alias, Directory, etc. Recordeu que el servei de correu des del punt de vista de recepció essencialment pot ser: local, dominis locals, com a smarthost. El correu des del punt de vista del lliurament essencialment pot ser: local, cap a smarthost, a internet. (1.5)

3. Actualment gairebé cap operador ofereix adreça IP pública (encara que sigui dinàmica) per a les connexions de dades mòbils (2G, 3G, 4G, etc.). Es vol disposar d'un petit sistema autònom amb bateries que faci de servidor de vídeo amb una webcam. Es viable que des de Internet es pugui accedir a aquest servidor?. Suposeu que el servei de vídeo es troba disponible gràcies a l'aplicació VLC que ofereix un streaming pel port 80. Doneu una solució tècnicament viable, si és possible, per aconseguir-ho. Enumereu els recursos que us calen des del punt de vista de l'assignatura ASI (registrar donimi, servidor a Internet, servidor a casa, tipus de servei instal·lat, etc.) (1)

4. Preguntes cert o fals. Justifiqueu la resposta. Les respostes incorrectes resten. Les respostes sense justificació compten la meitat. (4.5)

   a) És possible tenir més d'un servidor web en una xarxa privada i que el pugui accedir a ells amb diferents noms DNS només obrint únicament el port 80 de l'encaminador NAT que és l'únic que té l'adreça pública.

   b) Si la clau pública només s'envia a persones de confiança, es millora la seguretat de la privacitat dels missatges xifrats.

   c) Si la clau pública només es rep de persones de confiança, deixen de tenir sentit les autoritats certificadores.

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

   e) Si un client vol autentificar-se amb un servidor generant un parell de claus pública i privada, li ha de proporcionar 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.

   f) 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.

   g) Un missatge signat no és fiable si s'ha rebut per un canal que podem assegurar que no és fiable.

   h) El mecanisme més ràpid en qualsevol cas per distribuir el contingut de fitxers entre varis nodes és via peer to peer.

   i) Per a que un navegador web pugui presentar continguts en funció de l'usuari que s'hagi autentificat o les dades prèvies enviades, cal mantenir una comunicació http sempre oberta.

   j) Una comunicació http funciona per sobre d'una connexió TCP (generalment en el port 80). Aquesta connexió TCP es crea en cada petició http i es destrueix cada vegada que el navegador ha rebut tot el contingut que desitja mostrar.

   k) El mecanisme de Sockets permet el pas de missatges entre processos de diferents màquines però no entre processos de la pròpia màquina.

   l) Qualsevol comunicació que es faci utilitzant xarxes obertes com les de l'aeroport, etc. no pot ser segura.

   m) Les comunicacions fetes a través d'un proveïdor de Internet oficial (registrat com ISP) sempre són segures.

   n) Quan es compra un domini, el gestor al que li contractes l'únic que fa es demanar 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.

5. Proposa una solució al següent problema: Una petita empresa té la seva xarxa amb un adreçament privat. Disposa de un servidor web amb nom empresa.cat. Els empleats, a vegades estan a dins de la empresa (per tant el servidor web estarà a l'adreça 172.20.0.1) i a vegades es troben a fora de l'empresa amb un accés a Internet. L'encaminador NAT de l'empresa té com adreça pública la 83.5.5.5. Per tant, quan els usuaris obren un navegador amb http://empresa.cat volen veure el servidor estiguin on estiguin. Defineix quins serveis i quina configuració han de tenir per aconseguir això. (1)

6. Un mecanisme per obtenir un certificat vàlid de una autoritat certificadora per un servidor web amb nom empresa.cat consisteix en el següent: L'autoritat certificadora disposa de una web on es rep la petició del certificat. L'autoritat informa que envia un missatge de correu amb un codi a la bústia nom@empresa.cat on "nom" és escollit per la autoritat certificadora. La web espera fins que s'introdueix el codi rebut al missatge de correu. Si el codi coincideix, ofereix el certificat a qui l'ha demanat. (1)

   a) Consideres que és un mecanisme vàlid per concedir el certificat? Justifica.

   b) El contingut del missatge de correu a nom@empresa.cat, fa la funció de "nonce"?