Aplicacions i Serveis a Internet

durada 2h

Final - Juny 2014

1. Aplicant l'algoritme RSA, desxifreu el següent missatge: WQANÇADDKK. Teniu en compte que p=3, q=11 i e=3 (s'ha de trobar el valor correcte de d). (1.5)

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. Suposeu que teniu contractat un servei d'accés a Internet amb una única IP dinàmica. Disposeu també d'un domini estàtic bo.cat i d'un domini dinàmic dolent.nommassallargperquesiguiutil.cat. El gestor del domini estàtic us permet disposar d'un servidor web a on no es poden allotjar dades però sí qualsevol configuració. També us permet disposar d'un servidor de correu però no hi poden haver bústies on guardar cap missatge. Voleu muntar a casa els serveis de correu de manera que s'obtinguin les bústies de u1@bo.cat, u2@bo.cat, root@bo.cat i que la bústia de webmaster@bo.cat sigui la mateixa que root. A aquest servei de correu es vol accedir tant en mode de webmail amb l'adreça webmail.bo.cat com a través de IMAP amb imap.bo.cat. També ha de permetre accedir amb protocol SMTP a smtp.bo.cat. Per acabar d'arrodonir els serveis també es vol accedir al servei owncloud a través de nuvol.bo.cat.
   Dissenyeu de manera qualitativa la configuració d'aquests serveis. 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. (4)
   Es demana:
   a) Configuració de l'encaminador de la teva xarxa.
   b) Configuració del servei DNS justificant la vostra elecció. Definint quina part estarà en el gestor i quina part estarà a la vostra xarxa.
   c) Configuració del servei WEB justificant la vostra elecció. Definint quina part estarà en el gestor i quina part estarà a la vostra xarxa.
   d) Configuració del servei de correu justificant la vostra elecció. Definint quina part estarà en el gestor i quina part estarà a la vostra xarxa.

3. Què és un certificat d'usuari? Podem confiar en qualsevol certificat d'usuari vinguin d'on vingui? Quina característica fa que siguin fiables?

4. Dibuixa l'esquema tant de l'emissor com del receptor en el que es basa el correu segur per xifrar i signar els missatges.

5. En quina capa actua el servei DNS? Justifica.

6. Intentes connectar-te al servidor VPN i no funciona. Fas un ping a la seva adreça IP 147.83.101.75 i respon correctament però en canvi fas un ping al seu nom desword.epsem.upc.edu i no respon. On pot ser el problema? Quines altres proves faries per confirmar-ho?

7. Enumera totes les diferències entre fer servir el mètode GET o POST en un formulari. (1)

8. Quina seguretat ofereix servir un fitxer a algunes persones en concret mitjançant una URL del tipus /15799fitxersecret3333333/fitxer.pdf? Quina característica ha de tenir el servidor per a que un bot no el detecti?

9. Quina funció fa la suma demanada en els missatges de la pràctica de GPG? Es pot associar amb alguns dels conceptes explicats a les sessions de teoria? (1)