Aplicacions i Serveis a Internet

Seguretat

Final - Juny 2013

1. Aplicant l'algoritme RSA, desxifreu el següent missatge: RZLC_CNANÇ. Teniu en compte que p=3, q=11 i e=3 (s'ha de trobar el valor correcte de d). (2)

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. Enumera les funcions que s'han de protegir quan es parla de seguretat de la informació. (0.5)

3. Dibuixa l'esquema tant de l'emissor com del receptor en el que es basa el correu segur per xifrar i signar els missatges. (0.5)

4. Respon cert o fals. Les respostes incorrectes resten 0.5 (5.5)

   a) Un router amb el privilegi de poder filtrar paquets es considera un Firewall.

   b) Un Firewall és un dispositiu que pot actuar en tots els nivells de l'arquitectura de comunicacions per decidir si filtra les PDU corresponents.

   c) Els algoritmes de clau simètrica són més fàcils de trencar que els de clau pública.

   d) L'Autoritat de Certificació s'encarrega de signar la clau pública i privada d'un usuari per generar el certificat.

   e) Les Autoritats de Certificació són les úniques que podrien desxifrar els missatges en cas de requeriment justificat.

   f) Les pagines web segures són aquelles que fan servir el protocol https. Aquest protocol és totalment diferent al http i s'ha dissenyat des de zero per tenir en compte el xifrat.

   g) SSL es fa servir per oferir seguretat als protocols de web i de correu.

   h) Els algoritmes de seguretat basats en un algoritme ocult són sempre més segurs que els algoritmes públics, ja que aquests últims sempre es poden trencar amb temps i potència de càlcul suficients.

   i) Un usuari que no tingui generat el parell de claus pública i privada pot xifrar un missatge.

   j) Un usuari que no tingui generat el parell de claus pública i privada pot signar un missatge.

   k) Si un usuari envia un missatge xifrat a un altre amb clau pública, tant l'emissor com el receptor el poden desxifrar.

5. Defineix la funció d'un Firewall. Enumera els tipus de Firewalls i la seva relació amb la quantitat de recursos que necessiten. (0.5)

6. Descriu com funciona la capa SSL. Descriu com ofereix la confidencialitat, la integritat i la autenticació. Quantes classes de claus existeixen? (0.5)

7. Quines característiques ha de complir una bona funció de Hash per utilitzar-la com signatura. (0.5)