REDES DE COMUNICACIONES 2

25 de abril de 2014

Apellidos Nombre:

Preguntas	1	2	3	4	5	Total
Puntos	3	2	3	1	1	10
Calificación						

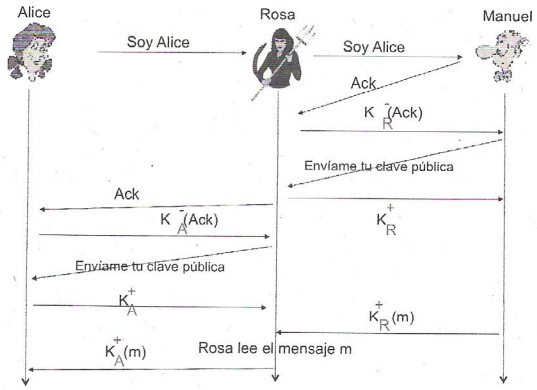
1) Utilizando el algoritmo RSA, con p=3, q=11 y e=9, codifique la palabra "Eloy" (utilizando la equivalencia de la tabla ASCII mostrada)

a) Carácter por carácter, en caso de ser posible. Si no posible explique por qué.

b) La palabra completa como un mensaje m, en caso de ser posible. Si no es posible explique por qué.

064d	40h	@	080d	50h	P	096d	60h	`	112d	70h	p
065d	41h	A	081d	51h	Q	097d	61h	a	113d	71h	q
066d	42h	B	082d	52h	R	098d	62h	b	114d	72h	r
067d	43h	C	083d	53h	S	099d	63h	c	115d	73h	s
068d	44h	D	084d	54h	T	100d	64h	d	116d	74h	t
069d	45h	E	085d	55h	U	101d	65h	e	117d	75h	u
070d	46h	F	086d	56h	V	102d	66h	f	118d	76h	v
071d	47h	G	087d	57h	W	103d	67h	g	119d	77h	w
072d	48h	H	088d	58h	X	104d	68h	h	120d	78h	x
073d	49h	I	089d	59h	Y	105d	69h	i	121d	79h	y
074d	4Ah	J	090d	5Ah	Z	106d	6Ah	j	122d	7Ah	z
075d	4Bh	K	091d	5Bh	[	107d	6Bh	k	123d	7Bh	{
076d	4Ch	L	092d	5Ch	\	108d	6Ch	l	124d	7Ch	|
077d	4Dh	M	093d	5Dh	]	109d	6Dh	m	125d	7Dh	}
078d	4Eh	N	094d	5Eh	^	110d	6Eh	n	126d	7Eh	~
079d	4Fh	O	095d	5Fh	_	111d	6Fh	o	127d	7Fh	⌂

2) Dado el siguiente ataque por interposición (man-in-the-middle)



¿Evitaría el ataque que Alice requiera que Manuel se autentique utilizando el protocolo de clave pública? Explique su razonamiento

3) Suponga que Alice quiere enviar un correo electrónico a Bob. Bob tiene una pareja de claves pública-privada (K_B^+, K_B^-) y Alice dispone del certificado de Bob. Pero Alice no tiene una pareja de claves pública-privada.

a) ¿Es posible diseñar un esquema mediante el que Bob pueda verificar que es Alice quien ha creado el mensaje utilizando SHA1? En caso afirmativo, describa el esquema mediante un diagrama de bloques para Alice y Bob. En caso negativo, esplique por qué no.

b)¿Es posible diseñar un esquema que proporcione confidencialidad para enviar el mensaje de Alicia a Benito? En caso afirmativo, describa el esquema mediante un diagrama de bloques para Alice y Bob. En caso negativo, esplique por qué no.

4) ¿Cuál es la diferencia importante entre un mensaje solicitud-respuesta y un mensaje TRAP en SNMP?

5) ¿Qué es un "motor SNMP" y qué función tiene?