REDES DE COMUNICACIONES 2

23 de mayo de 2017 – Parte 2

Apellidos Nombre:

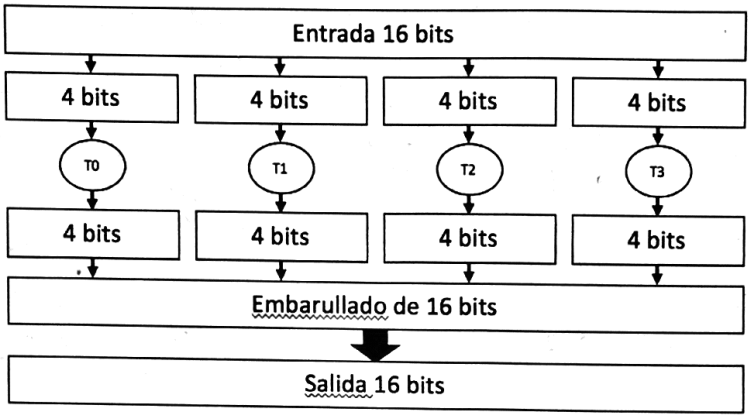
Preguntas	1	2	3	Total
Puntos	4	3	3	10
Calificación				

Pregunta 1) Utilizando el algoritmo RSA, con p=3, q=11 y e=7, codifique la palabra "mensaje" (utilizando la equivalencia de la tabla ASCII mostrada). Suponga (y describa) valores lógicos para todo dato faltante.

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	⌂

Mensaje transmitido:

Pregunta 2) Trend se ha enterado de que Alice y Bob se comunican utilizando cifrado de bloque ECB (Electronic CodeBook) para cifrar los mensajes. Asume que el algoritmo de cifrado deber funcionar en base al siguiente esquema:



Trend todavía no sabe qué hacen las funciones T0, T1, T2 y T3, ni cómo mezcla los bits la función de embarullado. Sin embargo, sí ha sido capaz de averiguar la codificación de ciertos textos en claro seleccionados, tal como se muestran en la siguiente tabla:

E	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
S	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**
E	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
S	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**
E	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
S	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**1**
E	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
S	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**
E	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
S	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**
E	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**
S	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
E	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**
S	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
E	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**
S	**0**	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
E	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**
S	**0**	**1**	**0**	**1**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

a) Explique razonadamente cuál será la salida dado el siguiente bloque de bits de entrada:

E	**1**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**0**
S																

b) Con la información disponible, ¿sería posible decodificar cualquier mensaje? Explique

Pregunta 3) Imagine una aplicación de software que quiere ofrecer reuniones virtuales seguras. Para ello los tres participantes, Alice, Bob y Carolina, poseen clave pública-privada. Entre otros aspectos, se requiere que cuando Alicia le manda un mensaje a Bob y a Carolina, se dé que:

a) Solo Bob y Carolina puedan leer el mensaje de Alicia.

b) Bob y Carolina tenga confianza en que el mensaje viene de Alicia y no ha sido alterado.

c) Bob y Carolina confían mutuamente entre sí, pero desconfían de Alicia. Entonces quieren tener la seguridad de que Alicia ha enviado exactamente el mismo mensaje a ambos.

Diseñe un protocolo seguro que basado en las claves público-privadas de los 3 participantes y cualquier otro elemento que considere necesario garantice las 3 condiciones descritas.