Comenzado el	Friday, 12 de May de 2023, 18:01
Estado	Finalizado
Finalizado en	Friday, 12 de May de 2023, 18:31
Tiempo empleado	30 minutos 35 segundos
Calificación	**9,25** de 10,00 (**93**%)

Información

MÓDULO 5. CRIPTOGRAFÍA DE CLAVE PÚBLICA

Pregunta 1

Correcta

Se puntúa 1,00 sobre 1,00

Antonio quiere mandar un mensaje $m = \mathrm{CRZ}$ a Bárbara a través de un canal no seguro. Para ello, deciden acordar que el algoritmo criptográfico a utilizar será RSA. Para pasarlo a código numérico, utilizaremos el siguiente alfabeto:

A B C D E F G H I J K L M N

01 02 03 04 05 06 07 08 09 10 11 12 13 14

O P Q R S T U V W X Y Z

15 16 17 18 19 20 21 22 23 24 25 26 00

Si sabemos que Bárbara elige la siguiente pareja de números primos: $p_{\text{Bárbara}} = 97$, $q_{\text{Bárbara}} = 101$, según el teorema de Euler, ¿podría enviar Antonio este mensaje a Bárbara? Elegid la explicación y justificación correcta.

Seleccione una:

a.
$m = 31826$ no es divisible ni por p ni por q, por tanto Antonio sí puede enviar el mensaje a Bárbara utilizando el método RSA. ✓

b.
$m = 31826$ es divisible por p y por q, por tanto Antonio sí puede enviar el mensaje a Bárbara a través del método RSA.

c.
$m = 31826$ no es divisible ni por p ni por q, por tanto Antonio no puede enviar el mensaje a Bárbara a través del método RSA.

d.
$m = 31826$ es divisible por p, pero no es divisible por q, por tanto Antonio sí puede enviar el mensaje a Bárbara por el método RSA.

Pregunta 2

Correcta

Se puntúa 3,00 sobre 3,00

Sabemos que Bárbara ha elegido la siguiente pareja de números primos: $p_{\text{Bárbara}} = 97$ y $q_{\text{Bárbara}} = 101$, podemos decir que:

1. ¿La opción $e_{\text{Bárbara}} = 359$ se puede considerar una clave pública?
2. ¿La opción $e_{\text{Bárbara}} = 357$ se puede considerar una clave pública?

Seleccione una:

a.
$e_{\text{Bárbara}} = 357$ se puede considerar una clave pública y $e_{\text{Bárbara}} = 359$ no se puede considerar una clave pública para $p_{\text{Bárbara}} = 97$ y $q_{\text{Bárbara}} = 101$ dados.

b.
Ni $e_{\text{Bárbara}} = 359$ ni $e_{\text{Bárbara}} = 357$ se pueden considerar claves públicas para $p_{\text{Bárbara}} = 97$ y $q_{\text{Bárbara}} = 101$ dados.

c.
$e_{\text{Bárbara}} = 359$ se puede considerar una clave pública y $e_{\text{Bárbara}} = 357$ no se puede considerar una clave pública para $p_{\text{Bárbara}} = 97$ y $q_{\text{Bárbara}} = 101$ dados. ✓

d.
$e_{\text{Bárbara}} = 359$ y $e_{\text{Bárbara}} = 357$ se pueden considerar las dos claves públicas para $p_{\text{Bárbara}} = 97$ y $q_{\text{Bárbara}} = 101$ dados.

Pregunta 3

Correcta

Se puntúa 1,00 sobre 1,00

En este ejercicio, Bárbara con $q_{\text{Bárbara}} = 229$ decide dar a conocer su clave pública $n_{\text{Bárbara}} = 51983$, $e_{\text{Bárbara}} = 233$ para que le enviemos mensajes cifrados con RSA. Si Antonio le quiere enviar el mensaje $m = \text{ADV}$ utilizando el cuadro del alfabeto:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
01	02	03	04	05	06	07	08	09	10	11	12	13	14
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**		
15	16	17	18	19	20	21	22	23	24	25	26	00	

a) (50% de la nota) ¿Qué mensaje codificado recibirá Bárbara?

b) (50% de la nota) ¿Qué clave privada usará Bárbara para descifrarlo?

Respuesta:

c = 41196 ✓

d = 47105 ✓

Pregunta 4

Correcta

Se puntúa 2,00 sobre 2,00

Alí $(p_{\text{Alí}} = 467, q_{\text{Alí}} = 503, e_{\text{Alí}} = 523)$ conoce la clave pública de Boris $(p_{\text{Boris}} = 487, q_{\text{Boris}} = 509, e_{\text{Boris}} = 541)$ y le quiere mandar un mensaje de forma que se asegure la máxima autenticidad y confidencialidad posible.

El mensaje que Alí quiere enviar a Boris es CLO. Para pasarlo a código numérico, utilizaremos el siguiente alfabeto:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
01	02	03	04	05	06	07	08	09	10	11	12	13	14

O	P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25	26	00	

Se pide:

a) (50% de la nota) encontrad el mensaje a encriptar CLO.

b) (25% de la nota) encontrad la clave privada de Alí.

c) (25% de la nota) encontrad la clave privada de Boris.

Respuesta:

$m =$ 031215

$c1 =$ 63515

$c2 =$ 232741

Pregunta 5

Parcialmente correcta

Se puntúa 2,25 sobre 3,00

Alí $(p_{\text{Alí}} = 467, q_{\text{Alí}} = 503, e_{\text{Alí}} = 523)$ conoce la clave pública de Boris $(p_{\text{Boris}} = 487, q_{\text{Boris}} = 509, e_{\text{Boris}} = 541)$ y quiere enviarle un mensaje de manera que se asegure la máxima autenticidad y confidencialidad posible.

El mensaje que Alí quiere enviar a Boris es BAFON. Para pasarlo a código numérico, utilizaremos el siguiente alfabeto:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
01	02	03	04	05	06	07	08	09	10	11	12	13	14
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	_	
15	16	17	18	19	20	21	22	23	24	25	26	00	

Encontrad el mensaje enviado a Boris separando el mensaje en bloque inferiores a n y marcad aquellas opciones que consideréis correctas:

Seleccione una o más de una:

- [ ] a. Para buscar máxima **CONFIDENCIALIDAD**, utilizaremos el método de la de firma digital. Para buscar **AUTENTICIDAD**, a continuación utilizaremos el métode RSA de la forma habitual.
- [ ] b. Para garantizar la **CONFIDENCIALIDAD**, utilizamos el proceso de desencriptación con la clave pública de Alí.
- [x] c. Para garantizar la **AUTENTICIDAD**, utilizamos el proceso de desencriptación con la clave privada de Alí. ✓
- [x] d. Para garantizar la **CONFIDENCIALIDAD**, utilizamos el proceso de encriptación con la clave pública de Boris. ✓
- [ ] e. El mensaje enviado a Boris podría ser $c = 4125246056$ con firma digital previa $s = 1300639324$.
- [ ] f. Para garantizar la **AUTENTICIDAD**, utilizamos el proceso de encriptación con la clave privada de Boris.
- [x] g. Para buscar máxima **AUTENTICIDAD**, utilizaremos el método de la firma digital. Para buscar **CONFIDENCIALIDAD**, a continuación utilizaremos el método RSA de la forma habitual. ✓
- [ ] h. El mensaje enviado a Boris podría ser $c = 1300639324$ con firma digital previa $s = 4125246056$.

◄ CUESTIONARIO DE ENTRENO DEL MÓDULO 5 Criptografía de clave pública

Ir a...

Recursos complementarios externos - Módulo 5 Criptografía de clave privada ►