Comenzado el	martes, 14 de abril de 2020, 12:36
Estado	Finalizado
Finalizado en	martes, 14 de abril de 2020, 14:23
Tiempo empleado	1 hora 46 minutos
Puntos	11,00/11,00
Calificación	**10,00** de 10,00 (**100**%)

Pregunta 1

Correcta

Puntúa 1,00 sobre 1,00

Supongamos que los usuarios A y B llevan a cabo una distribución de clave secreta con el protocolo de Diffie-Hellman. Los valores que utilizan son p = 1087 , α = 3 , a = 724 y b = 512. Encontrad cual es el secreto que acabarán compartiendo.

Respuesta: 829 ✓

La respuesta correcta es: 829

Pregunta 2

Correcta

Puntúa 1,00 sobre 1,00

Arthur, Ford, Zaphod y la Trillian se han creado un par de claves RSA cada uno y han publicado sus claves públicas en un repositorio. Marvin ha conseguido descubrir los valores privados *d* de todos ellos, pero no es capaz de saber de quién es cada clave (ser un robot tiene sus limitaciones).

¿Podrías ayudarlo uniendo las claves públicas con sus respectivas claves privadas?

Ford: (nb,eb)=(1247,17) d=(761) ✓

Zaphod: (nc,ec)=(437,31) d=(115) ✓

Arthur: (na,ea)=(17819,4331) d=(4067) ✓

Trillian: (nd,ed)=(2701,1513) d=(1081) ✓

La respuesta correcta es: Ford: (nb,eb)=(1247,17) → d=(761), Zaphod: (nc,ec)=(437, 31) → d=(115), Arthur: (na,ea)=(17819,4331) → d=(4067), Trillian: (nd,ed)=(2701, 1513) → d=(1081)

Pregunta 3

Correcta

Puntúa 1,00 sobre 1,00

Dado el par de clave pública $(n_b, e_b) = (6767, 1261)$ y privada $(n_b, d_b) = (6767, 1141)$, consideremos el mensaje cifrado 5402. Nosotros sabemos que el mensaje original era 6877, pero al intentar descifrarlo no lo obtenemos. ¿Por qué no somos capaces de encontrar el mensaje original?

Seleccione una:

- a. El mensaje escogido no está en el grupo Zn en el que estamos trabajando ✓

Exacto. Si normalizamos el mensaje original a $\mathbb{Z}^*_{6767}$ encontraríamos $6877 \bmod 6767 = 5402$, que es el mensaje que hemos obtenido al descifrar

- b. Ninguna de las otras respuestas es cierta
- c. El módulo escogido no es primo
- d. El valor m que queremos cifrar no es coprimo con el módulo n
- e. No lo hemos descifrado correctamente (si realizamos el proceso inverso y realizamos el proceso de descifraje correctamente, obtendremos nuestro m inicial)

La respuesta correcta es: El mensaje escogido no está en el grupo Zn en el que estamos trabajando

Pregunta 4

Correcta

Puntúa 1,00 sobre 1,00

Un usuario debe responder la pregunta de una encuesta enviando su respuesta cifrada con la siguiente clave pública del criptosistema RSA (n,e)=(259, 85). La respuesta puede ser una de las siguientes: A, B, C y D. En el escenario planteado la pregunta y las respuestas posibles son públicas, pero las respuestas de los usuarios deben ser secretas.

El usuario envía el criptograma siguiente c= 68. El criptograma corresponde al cifrado, mediante la clave pública mencionada, del código ASCII de una de las opciones posibles. La tabla siguiente muestra los códigos ASCII de las opciones:

A - 65
B - 66
C - 67
D - 68

¿Puede un atacante, sin conocer la clave privada correspondiente, deducir cuál es el valor que el usuario ha respondido? En caso afirmativo, responded con la respuesta en claro enviada (A, B, C o D). En caso negativo, responded NO.

Respuesta:

D

La respuesta correcta es: D

Pregunta 5

Correcta

Puntúa 1,00 sobre 1,00

Los usuarios A y B se disponen a utilizar el sistema RSA para intercambiarse información. El usuario A ha escogido n_A=3827 y e_A=3125 ; el usuario B ha escogido n_B=1271 y e_B=689 .
El usuario A desea enviar su edad m=12 cifrada a B. Calculad el criptograma *c* que el usuario A enviará al usuario B.

Respuesta:

1036

La respuesta correcta es: 1036

Pregunta 6

Correcta

Puntúa 1,00 sobre 1,00

Los usuarios Alice y Bob se disponen a utilizar el sistema RSA para **firmar** los mensajes que se envían. Alice tiene la clave pública (n_a, e_a)=(10403, 8677) y la clave privada (n_a,d_a)=(10403,7213). Bob tiene la clave pública (n_b, e_b)=(1411, 1065) y la clave privada (n_b,d_b)=(1411,409).

Alice envía el mensaje m=382 firmado a Bob. ¿Cuál es la firma de Alice sobre este mensaje?

Respuesta:

5219

La respuesta correcta es: 5219

Pregunta 7

Correcta

Puntúa 1,00 sobre 1,00

Dos usuarios A y B, se intercambian mensajes con el sistema de clave pública ElGamal sobre el grupo multiplicativo $\mathbb{Z}_{97}^*$ con α=90. El usuario A envía a B el mensaje m= 43 . La clave privada de A es a= 44 y la clave pública es α^a=93.
¿Cuál (o cuáles) de las siguientes firmas son firmas válidas del mensaje m realizadas por el usuario A?

Nota: Las firmas son pares de valores, [r,s] .

Seleccione una o más de una:

- [x] a. [82,43] ✓
- [ ] b. [89,34]
- [ ] c. [70,56]
- [ ] d. [39,82]
- [x] e. [21,77] ✓
- [x] f. [71,75] ✓

Las respuestas correctas son: [82,43], [71,75], [21,77]

Pregunta 8

Correcta

Puntúa 1,00 sobre 1,00

Dos usuarios A y B se intercambian mensajes con el sistema de clave pública de ElGamal sobre un grupo multiplicativo $\mathbb{Z}_{71}^*$. La clave privada de B es b=33. ¿Cuál es la clave pública del usuario B si α=62?

Respuesta:

7

La respuesta correcta es: 7

Pregunta 9

Correcta

Puntúa 1,00 sobre 1,00

Considerad el criptosistema ElGamal, del cual conocemos el fichero público calculado a partir del elemento α=88 de $\mathbb{Z}_{103}$. El usuario A ha construido su clave pública como $\alpha^{27} = 39 \ mod \ 103$. Si sabemos que el par $(\alpha^y, c) = (66,34)$ es el resultado de cifrar el mensaje *m* con la clave pública del usuario A, ¿cuál es el mensaje original *m*?

Respuesta:

1

La respuesta correcta es: 1

Pregunta 10

Correcta

Puntúa 1,00 sobre 1,00

Dos usuarios A y B, se intercambian mensajes con el sistema de clave pública ElGamal sobre el grupo multiplicativo $\mathbb{Z}_{223}^*$ con $\alpha = 46$. El usuario A envía a B el mensaje *m*= 66. La clave privada de A es *a*=38 y la clave pública es α^a=213. Para enviar el mensaje, A ha escogido al azar *h*=197.

¿Cuál es la firma [r,s] que recibirá B?

Nota: Respectad el formato indicado para dar la solución. Es decir, dad los dos valores en una lista: *[r,s]* .

Respuesta:

[93,192]

La respuesta correcta es: [93,192]

Pregunta 11

Correcta

Puntúa 1,00 sobre 1,00

Un usuario tiene que responder la pregunta de una encuesta enviando su respuesta cifrada con la siguiente clave pública del criptosistema ElGamal (p,α,α^b)=(3313, 541 , 1943). La respuesta puede ser una de las siguientes: A, B, C y D. En el escenario planteado, la pregunta y las respuestas son públicas, pero las respuestas de los usuarios tienen que ser secretas.

El usuario envía el criptograma siguiente (785,277). El criptograma corresponde al cifrado con la clave pública mencionada del código ASCII de una de las opciones posibles. La tabla siguiente muestra los códigos ASCII de las opciones:

A - 65
B - 66
C - 67
D - 68

¿Puede un atacante, sin conocer la clave privada correspondiente y aprovechando el hecho que conoce los posibles valores que pueden ser cifrados, deducir cúal es el valor que el usuario ha respondido? En caso afirmativo, ¿cuál es la respuesta envíada?. En caso negativo, contestad no.

Seleccione una:

- a. No ✓
- b. B
- c. A
- d. D
- e. C

La respuesta correcta es: No

◄ PEC3 Ir a... PEC5 ►