Comenzado el	viernes, 29 de marzo de 2024, 11:25
Estado	Finalizado
Finalizado en	viernes, 29 de marzo de 2024, 11:28
Tiempo empleado	3 minutos 6 segundos
Puntos	3,00/3,00
Calificación	**10,00** de 10,00 (**100**%)

Pregunta 1

Correcta

Se puntúa 1,00 sobre 1,00

Si Alice cifra el mensaje m=16 con el criptosistema de ElGamal para enviarlo a Bob, quien utiliza como clave pública (p, a^x(mod p), a)= (23, 19, 5), ¿cuál de las siguientes parejas {K,C} es correcta?

Seleccione una:

a. {11, 10}
b. {22, 11}
c. {16, 3} ✔
d. {10, 11}

La respuesta correcta es: {16, 3}

Pregunta 2

Correcta

Se puntúa 1,00 sobre 1,00

Considerando los últimos tres dígitos del alu (alu1, alu2 , alu3), por ejemplo si alu= 1457652, entonces alu1 = 6, alu2 = 5, alu3 = 2 y
Alice desea enviar el mensaje m = alu1 + alu2 + alu3 a Bob.
El criptosistema utilizado es el de ElGamal con los siguientes parámetros: un número primo p = 31 y un elemento primitivo a = 3.
Alice, cuyo valor privado es 7 y cuyo valor público es 17, desea enviar el mensaje m a Bob, quien tiene valor público 16. ¿Cuál es el mensaje cifrado C enviado de Alice a Bob?

Seleccione una:

a. 12
b. 17
c. 11 ✔
d. 7

La respuesta correcta es: 11

Pregunta 3

Correcta

Se puntúa 1,00 sobre 1,00

En el criptosistema de ElGamal, suponiendo que Alice tiene clave privada kA envía un mensaje cifrado C=K *m (mod p) a Bob, con entero privado xB ¿cómo descifra Bob el mensaje recibido?

Seleccione una:

- a. m = (C * K^(-kA)) (mod p)
- b. m = (C * K^kA) (mod p)
- c. m = (C * K^xB) (mod p)
- d. m = (C * K^(-1)) (mod p) ✔

La respuesta correcta es: m = (C * K^(-1)) (mod p)