Comenzado el	martes, 9 de abril de 2024, 21:05
Estado	Finalizado
Finalizado en	miércoles, 10 de abril de 2024, 20:52
Tiempo empleado	23 horas 47 minutos
Calificación	**10,00** de 10,00 (**100**%)

Pregunta 1

Correcta

Se puntúa 10,00 sobre 10,00

Indica cuáles de las siguientes afirmaciones son ciertas sobre Criptografía de Curvas Elípticas:

Seleccione una o más de una:

- [ ] a. Una clave de 1024 bits para CCE equivale a una de 160 bits para RSA.
- [x] b. (7,9) es un punto de la curva y^2 = x^3 + x + 6 sobre GF(11). ✔
- [x] c. Hay que codificar los mensajes originales como puntos. ✔
- [x] d. Lo que en el PLD es un producto, en el PLD Elíptico es una suma. ✔
- [ ] e. La criptografía simétrica usa claves el doble de largas que la CCE.
- [x] f. Para calcular el múltiplo de un punto se usa la recta tangente a la curva en ese punto. ✔
- [x] g. Las operaciones son más lentas que las usadas en los sistemas basados en factorización. ✔
- [x] h. El número de puntos debe tener un factor primo grande. ✔
- [ ] i. (6,8) es un punto de la curva y^2 = x^3 + x + 6 sobre GF(11).
- [x] j. El NIST no debe recomendar curvas elípticas concretas. ✔
- [ ] k. El resultado del criptosistema elíptico de ElGamal es un punto.
- [x] l. Los ataques actuales a CCE se basan en las ejecuciones de los programas. ✔
- [ ] m. Lo que en el PLD Elíptico es una potencia, en el PLD es un producto.
- [ ] n. La suma de puntos coincide con la intersección de la recta que los atraviesa y la curva.

Las respuestas correctas son: Lo que en el PLD es un producto, en el PLD Elíptico es una suma., Para calcular el múltiplo de un punto se usa la recta tangente a la curva en ese punto., (7,9) es un punto de la curva y^2 = x^3 + x + 6 sobre GF(11)., Hay que codificar los mensajes originales como puntos., Las operaciones son más lentas que las usadas en los sistemas basados en factorización., El número de puntos debe tener un factor primo grande., El NIST no debe recomendar curvas elípticas concretas., Los ataques actuales a CCE se basan en las ejecuciones de los programas.