Comenzado el	viernes, 29 de marzo de 2024, 11:56
Estado	Finalizado
Finalizado en	viernes, 29 de marzo de 2024, 12:16
Tiempo empleado	19 minutos 53 segundos
Puntos	1,00/1,00
Calificación	**10,00** de 10,00 (**100**%)

Pregunta 1

Correcta

Se puntúa 1,00 sobre 1,00

Señale las afirmaciones que son ciertas sobre cifrados de clave pública:

Seleccione una o más de una:

- [ ] a. En RSA deben usarse tablas de números pseudoaleatorios publicadas
- [ ] b. Clifford Cocks patentó el algoritmo RSA en 1983
- [x] c. PKCS se refiere a un grupo de estándares de criptografía de clave pública ✔
- [x] d. El problema del logaritmo discreto sobre curvas elípticas es intratable ✔
- [x] e. En RSA nunca se debe compartir módulos n con otros usuarios ✔
- [x] f. El Teorema de Euler garantiza la recuperación del mensaje original en el RSA ✔
- [x] g. Si se usan p y q cercanos puede atacarse el RSA usando la raíz cuadrada de n ✔
- [ ] h. Una función unidireccional es una transformación de fácil inversión
- [ ] i. Cada usuario tiene una clave privada para cifrar y una clave pública para descifrar
- [ ] j. La mayoría de criptosistemas simétricos son mucho más lentos que RSA

Las respuestas correctas son: El problema del logaritmo discreto sobre curvas elípticas es intratable, El Teorema de Euler garantiza la recuperación del mensaje original en el RSA, PKCS se refiere a un grupo de estándares de criptografía de clave pública, Si se usan p y q cercanos puede atacarse el RSA usando la raíz cuadrada de n, En RSA nunca se debe compartir módulos n con otros usuarios