

Facultat d'Informàtica de Barcelona
Examen final de Criptografia
23 de juny de 2009

1. Describe el modo de operación CBC y señala dos diferencias con el modo COUNTER.
2. Los usuarios A y B comparten el mismo módulo n para un RSA, y tienen exponentes respectivos e_A y e_B tales que $\text{mcd}(e_A, e_B) = 1$. Supongamos que alguien envía el mismo mensaje m cifrado a ambos usuarios. Demuestra que si se interceptan los criptogramas c_A y c_B se puede obtener el mensaje m .
3. Sea p un número primo y a un número entero positivo no divisible por p . Considera la función

$$H(x) = a^x \text{ mod } p.$$

Analiza si esta función es

- a) eficientemente calculable b) unidireccional c) libre de colisiones

¿Puede usarse como función hash?

4. Certificados digitales: utilidad, contenido y formato.

Cada pregunta 1.5 puntos

Las notas se publicarán en el Racó el día 25 de junio

La revisión (del examen y las prácticas) será el día 26, a las 13h. en el despacho 338 del edificio Omega