Ayudantía 10

IIC3253 - Criptografía y Seguridad Computacional

Christian Klempau

1 Repaso

1.1 Esquematice los pasos necesarios a ejecutar e intercambios de información en las firmas usando RSA

1.2 Defina en detalle qué hace A y B para la firma de Schnorr, y demuestre la correctitud del algoritmo

1.3 ¿Cómo se define un Grupo? ¿Qué requisitos debe tener el operador?

2 Teorema de Lagrange y grupos generadores

Dado el teorema de Lagrange:

Sea G un grupo finito y H un subgrupo de G. Entonces el orden de H divide al orden de G.

Dado el siguiente grupo finito: $\mathbb{Z}_{10}^* = (\{1, 3, 7, 9\}, *\mod 10)$

¿Cuáles son sus subgrupos? Demuestre matemáticamente y compruebe que se cumple el teorema de Lagrange.

3 Schnorr: Efficient Signature Generation by Smart Cards

Describa en detalle el algoritmo y el funcionamiento de KAC descrito en el paper:

`https://d-nb.info/1156214580/34`

3.1 ¿Qué hace el verificador y qué hace el usuario?

3.2 Describa el protocolo, paso a paso

3.3 Demuestre su correctitud