

Criptografía y Seguridad (72.04)

TRABAJO PRÁCTICO DE IMPLEMENTACIÓN: SECRETO COMPARTIDO EN IMÁGENES CON ESTEGANOGRAFÍA

1 Cuestiones a analizar.

Deberán analizarse las siguientes cuestiones:

1. Discutir los siguientes aspectos relativos al documento.
 - a. Organización formal del documento.
 - b. La descripción del algoritmo de distribución y la del algoritmo de recuperación.
 - c. La notación utilizada, ¿es clara? ¿cambia a lo largo del documento? ¿hay algún error?
2. ¿Por qué la propuesta de Azzahra y Sugeng supone una mejora a la propuesta de Li Bai?
3. ¿Qué dificultades se encuentran al elegir pares (k, n) distintos de los establecidos en este TP?
4. ¿Por qué es importante controlar el rango de A y el resultado de $A^t \cdot A$?
5. ¿Por qué es válida la forma de generar los X_i ?
6. La imagen RW que se obtiene es una imagen “con ruido”. ¿Sería necesario ocultarla mediante esteganografía? ¿Cómo podría hacerse?
7. ¿Por qué siempre hay que indicar n , aún al recuperar?
8. ¿En qué otro lugar puede guardarse el número de sombra?
9. ¿Por qué hay
10. Discutir los siguientes aspectos relativos al algoritmo implementado:
 - a. Facilidad de implementación
 - b. Posibilidad de extender el algoritmo o modificarlo.
11. ¿En qué situaciones aplicarían este tipo de algoritmos?