**UNIVERSIDAD NACIONAL DE JUJUY - FACULTAD DE INGENIERÍA**

**INGENIERÍA INFORMÁTICA – LICENCIATURA EN SISTEMAS**

**SEGURIDAD Y AUDITORIA INFORMATICA**

**TRABAJO PRÁCTICO Nº 4. ESTEGANOGRAFIA, CRIPTOGRAFÍA Y FIRMA DIGITAL**

1. En un sistema criptográfico, cuando se habla de mensaje M ¿A que hace referencia?
2. ¿Qué tipo de archivo se puede usar como contenedor en esteganografia?
3. En los criptosistemas clásicos ¿Qué se debía mantener en secreto para obtener la confidencialidad?
4. En criptografía simétrica ¿Es necesario mantener en secreto el funcionamiento del algoritmo? ¿Por qué?
5. ¿Cuáles son los inconvenientes de la criptografía simétrica?
6. ¿Qué tipos de desventajas tiene la criptografía asimétrica?
7. ¿Es fácil calcular el inverso de una función hash? Justifique.
8. ¿En qué radica la seguridad del algoritmo RSA?
9. ¿Qué tipo de criptografía permite el desarrollo de la firma digital?
10. ¿Qué se busca resguardar con la firma digital?
11. ¿Con que se soluciona el problema de distribuir claves públicas de manera fiable?
12. Si el emisor cifra un mensaje con su clave privada usando criptografía asimétrica ¿Qué se obtiene?
13. ¿En los sistemas de clave pública se puede cifrar gran cantidad de datos? ¿Por qué?
14. ¿Cómo se puede saber si la clave pública de un usuario es suya y no la de un impostor?
15. Explique de manera breve el funcionamiento del algoritmo AES.
16. Instale el programa Gpg4win disponible en <https://www.gpg4win.org/>, genere el par de claves. Un integrante por grupo deberá subir su clave pública en la tarea denominada “Recepción de claves públicas” del aula virtual.
17. Descargue el programa llamado OpenStego disponible en <https://www.openstego.com/>. Como calificación de la tarea “Recepción de claves públicas” del punto anterior, recibirá un estego-objeto y una clave encriptada. Use el programa Gpg4win para des encriptar la clave. Luego use esta clave en el programa OpenStego junto al estego-objeto y obtenga el texto escondido. Copie el texto en este punto.
18. Suba este trabajo practico encriptado usando criptografía asimétrica. La clave pública del profesor se encuentra en el aula virtual.