PROYECTO DEL PRIMER PARCIAL

Seguridad informática y análisis forense SIS4403

El proyecto consiste en que cada alumno deberá realizar las siguientes actividades:

EJERCICIO1:

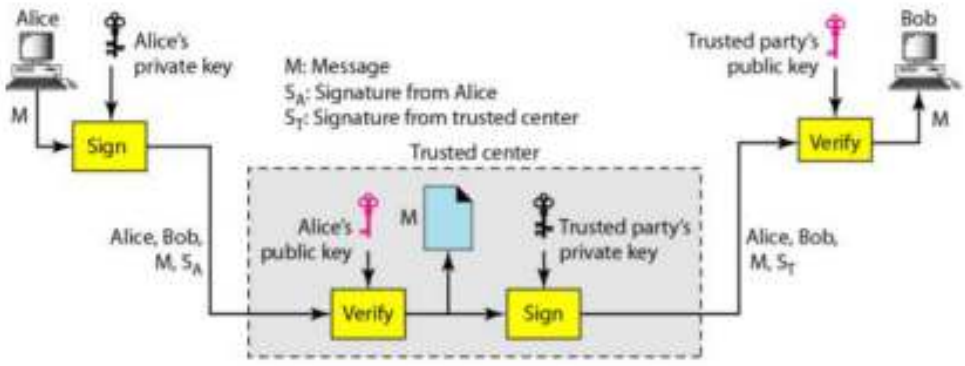
El alumno deberá utilizar el algoritmo RSA para que Alice le mande un mensaje cifrado a Bob con las siguientes características.

- El mensaje “M” será de 1050 caracteres.
- El alumno deberá generar h(M) para una vez descifrado constatar la autenticidad del mensaje M.
- Por cuestiones de eficiencia el alumno deberá dividir en partes más pequeñas de 128 caracteres el mensaje antes de ser cifrado y enviado.
- Alice cifrará los mensajes producto de la división del mensaje original con la llave pública de Bob.
- Bob descifrará los mensajes con su llave privada y con cada uno de ellos obtendrá el mensaje original de 1050 caracteres.
- Bob generará el hash del mensaje recibido h(M’).
- Debemos comparar si h(M) = h(M’)

EJERCICIO2:

Mediante el algoritmo RSA Alice firmará digitalmente el contrato NDA.pdf que se adjunta en la actividad, deberá cumplir con las siguientes instrucciones:

- Alice firmará digitalmente el contrato h(M) usando el algoritmo RSA mediante su llave privada.
- Una vez obtenida la firma Alice agregará dicha firma (cadena de caracteres) al archivo PDF y se lo enviará a la Autoridad Certificadora (AC).
- La AC obtendrá el HASH del documento original y verificará la firma usando la llave pública de Alice.
- La AC firmará el documento con su llave privada y se la agrega al PDF y se la envía a Bob.
- Bob obtiene el HASH del documento PDF y verifica la firma de la AC con la llave pública de AC.



PREGUNTAS:

1. Describir la importancia del método RSA en el contexto del protocolo https.
2. Describa en que consiste la capa 7 del modelo OSI y cuáles son los principales ataques a dicha capa.
3. Describe cuál es la importancia del algoritmo RSA en tus propias palabras.
4. ¿Qué uso le darías en la vida real al cifrado asimétrico usando RSA?
5. Describe cuál es la importancia de la ciberseguridad en nuestro entorno y como debemos protegernos.

INTRUCCIONES ADICIONALES:

1. Para los ejercicios 1,2 para “e” usaremos el número 4 de Fermat.
2. Para los primos usaremos números aleatorios de 1024 bits.

ENTREGABLES:

1. Para los ejercicios 1,2 deberán crear un repositorio.
2. En la actividad deberán subir un archivo PDF con capturas de pantalla de los resultados de los ejercicios 1,2, así como, el link de sus repositorios y las respuestas a las preguntas y sus conclusiones, el PDF debe venir con una portada.