Tarea 1 de Programación Curso: Seguridad Informática - Semestre 2017/2

Objetivo Tarea :

Alumno aprenda el manejo de conceptos de criptografía simétrica y de llave publica y del API disponible en Java para su uso.

Enunciado Tarea:

Esta tarea es INDIVIDUAL. Usted desea intercambiar a través de email un mensaje secreto con otro compañero del curso (usted lo selecciona). Para ello usted debe de crear un archivo de texto y cifrarlo con criptografía simétrica. La llave secreta empleada debe ser incluida en el archivo de tal modo que su compañero sea el único que pueda conocerla. Ademas su mensaje debe de incluir su firma digital (criptografía asimétrica), de modo que su compañero pueda comprobar que usted creo el mensaje.

Basado en los códigos de programación basados en criptografía simétrica y de llave publica que están disponibles en Piazza, se le pide que:

1. Crear con la herramienta KeyTool un par de llaves publica y privada del tipo RSA. Extraiga un certificado en formato X509 que contenga su llave publica y luego envíelo por email al profesor para que lo publique en Piazza.

2. Parte I : Usted debe de desarrollar un programa en java que permita:

    1. Generar una llave de sesión para encriptar con AES un archivo de texto de largo arbitrario cuyo contenido usted decida (es el que enviara a su compañero). UTILICE MODO CBC. No se permite uso del modo EBC. Por tanto deberá generar un vector de inicialización (IV).

    2. Generar Hash del Mensaje con SHA-1.

    3. Encriptar (RSA) llave de sesión con llave publica de su compañero. Como se indico esta llave publica debería estar en un certificado X509 y disponible en Piazza. Si no, solicite a su compañero que envíe certificado al profesor.

    4. Firme digitalmente el hash del mensaje. Utilice la KeyTool para acceder a su llave privada.

       Considere el siguiente orden estricto (por compatibilidad) de los datos escritos en el archivo de salida:

        - IV (en texto plano)
        - $E_{RSA}(K_{sesion}, K_{publica\_compañero})$
        - $E_{RSA}(Hash(Mensaje), K_{su\ llave\ privada})$
        - $E_{AES}(Mensaje,\ K_{sesion})$

    5. Si usted sigue tal orden su compañero debería ser capaz de decodificar su mensaje sin problemas y este deberá enviarle un mensaje de respuesta por email siguiendo el mismo formato.

       Parte II: Para poder decodificar el archivo que le envió su compañero

desarrolle un programa que realice lo siguiente:

1. Recuperar la llave de sesión encriptada en el archivo y la firma digital del mensaje. Para ello, averigüe cuales son el tamaño de un vector de inicialización, de una llave de sesión encriptada con AES y del tamaño de un hash (use solo SHA-1, aunque sabemos que no es seguro), Utilice estos datos para crear arreglos de bytes para recuperar estos datos.
2. Lea el vector IV, el cual debe ir en texto plano.
3. Desencriptar llave de sesión con su llave privada. Usted puede recuperar su llave con la KeyTool.
4. Desencriptar archivo con la llave de sesión. Si esto no es posible muestre mensaje de error en pantalla.
5. Calcular el Hash del mensaje desencriptado.
6. Validar firma del profesor. Esto se realiza comparando el hash extraído de la firma con el hash del mensaje, Si estos son iguales entonces la firma digital es valida y por tanto el mensaje es autentico.

Indicación: Averigüe el uso del método *available()* de la clase Java *FileInputStream*, Este método podría ayudarle a saber que cantidad de bytes le quedan por leer de un archivo. Asuma que el archivo enviado por su compañero sigue el mismo orden establecido para el archivo que usted le envió a el. Puede utilizar como base los códigos vistos en clases y publicados en Piazza.

Detalles envío Tarea y Revisión de su Tarea:

Partes I Y II:
Envié al profesor por email un archivo compacto con el siguiente nombre:

- *tarea1_seguridad_Informática_Apellido_y_nombre_alumno.zip*
- *El asunto de su email DEBE SER Tarea 1 Seguridad Informática 2017/2*

Este archivo compacto debe incluir lo siguiente:

- Código fuente java programas parte I y II
- En archivo de texto que envió a su compañero
- El archivo de texto encriptado recibido de su compañero
- El archivo de texto descifrado de su compañero

Para evaluar su tarea se considerara:

1. *El envío por email de su llave publica en certificado para que profesor lo publique en Piazza*
2. *Decodificación correcta del mensaje enviado por su compañero.*
3. *Compilación y ejecución correcta del código que encripta mensajes*
4. *Compilación y ejecución correcta del código que desencripta mensajes*
5. *Mensaje enviado a su compañero en texto plano y cifrado*
6. *Verificación de la autoría de un mensaje.*

Para determinar la nota de su tarea debe acordar un horario de revisión (10 mins) con el profesor. Si esta revisión no se realiza/agenda a mas tardar al mediodía del 15 de diciembre del 2017, su tarea sera evaluada con la nota mínima (1.0), aun cuando HAYA ENVIADO SU CORREO.