Laboratorio 2 – Criptografía en Java
Seguridad Informática

Indicaciones Generales
Redacte en un documento las respuestas a los puntos requeridos a continuación haciendo uso del material disponible en Moodle.

Indicaciones:

- Actividad en Parejas.
- Registro del avance en clases de manera individual.

Desarrollo:

Parte 1:

1. Analice objetivo de la herramienta KeyTool y forma de uso.

2. Respecto de la herramienta KeyTool, indique lo que realizan los comandos:

- keytool -genkey -keyalg RSA -keypass password -alias mykey -storepass storepass -keystore myKeyStore.jks

- keytool -list -v -keystore myKeyStore.jks

- keytool -export -alias mykey -file mycert.cer -keystore myKeyStore.jks

Cree, con la herramienta KeyTool, un par de claves pública y privada del tipo RSA.

Parte 2:

1. Desde Moodle, descargue la clase EncryptWithKeyStore.java. Realice los ajustes necesarios para hacer uso de las claves almacenadas en su keyStore. Ejecute la clase. ¿Qué se generó? Construya una clase Decrypt.java que permita obtener el texto plano original.

2. Cree una clase donde genere hash de un mensaje almacenado en un archivo de texto usando MD5 o SHA-1. Luego, encripte la salida resultante con su clave privada. ¿Qué características de seguridad se logran con lo realizado?

3. Cree una clase donde genere una clave de sesión para encriptar con AES un archivo de texto de largo arbitrario. Encripte el resultado con clave pública de un compañero, envíe archivo a su compañero.

4. Cree una clase que reciba el archivo encriptado, generado en 2, y muestre texto claro.

5. Suba las clases a Moodle.