Objetivo

Representar los conceptos relacionados con garantizar la confidencialidad en una comunicación usando la infraestructura de clave pública. Al terminar este taller, el estudiante estará en la capacidad de desarrollar una aplicación de intercambio de archivos de forma segura y utiliza certificados digitales.

Descripción del caso

Anastasia y Bonifacio son dos estudiantes de diseño quienes están trabajando desde hace más de un año en un proyecto súper innovador que puede ser financiado y les permitirá desarrollar su iniciativa de negocio. Ahora con el confinamiento obligatorio, ordenado por el COVIT-19, no pueden reunirse y trabajar juntos como lo hacían todas las tardes en la biblioteca de la Universidad. Ellos requieren una forma segura de intercambio de los archivos del proyecto. Anastasia estudió las condiciones de uso de los servicios de intercambio de archivos más utilizados como DeadBox o TwoDrive y encontró que si aceptan el uso deberán permitir que sus archivos sean escaneados, leídos y analizados. No quieren correr ningún riesgo de que su idea, y su trabajo sea espiado por las empresas de Silicone Valley. Bonifacio conoce a dos estudiantes del curso de Seguridad Informática quienes pueden construir un sistema de intercambio seguro de archivos basado en infraestructura de clave pública. Los estudiantes saben que Bonifacio está desarrollo un proyecto con potencial y desean hacer parte del emprendimiento. Anastasia y Bonifacio aceptan y disponen una participación para los estudiantes de Seguridad Informática por sus valiosos aportes al proyecto.

La secuencia de actividades propuesta es la siguiente:

Si Anastasia quiere enviar un archivo a Bonifacio se ejecutan las siguientes seis tareas:

1. Bonifacio crea un par de claves, una pública y otra privada.
2. Bonifacio envía a Anastasia su clave pública.
3. Anastasia utiliza la clave pública de Bonifacio para cifrar el archivo.
4. Anastasia envía el archivo cifrado a Bonifacio por la red insegura.
5. Bonifacio recibe el archivo cifrado.
6. Bonifacio descifra el archivo utilizando su clave privada.

Dado que Bonifacio no es estudiante de Informática y que no conoce de estos temas de seguridad, solicita que la aplicación sea muy simple, que tenga únicamente dos entradas: el archivo que se requiere enviar y el archivo de la clave pública, y genera el archivo asegurado. La aplicación del receptor ende deberá cargar el archivo asegurado, la clave privada y generar el archivo descifrado.

Desarrollo

Para cada una de las tareas de este taller se seguirá la Java™ Cryptography Architecture[1]. Adicionalmente se recomienda leer la Guia de programación de Java[2]. La aplicación tiene tres funcionalidades crea las claves pública y privada, el modo de cifrado y el de descifrado de archivos.

Crear un par de claves

1. Utilice la biblioteca KeyFactory para la generación de claves públicas y privadas. Es necesario que se almacene cada una de las claves en archivos individuales para facilitar el uso. Especialmente la clave pública en formato PEM.

Cifrado de archivo con clave pública

2. Utilice la clave pública recibida para el cifrado del archivo que desea proteger. La aplicación recibe el archivo y la clave pública, pueden ser las rutas o por medio de un FileChooser. Este módulo construye un archivo cifrado.

Descifrado del archivo con clave privada

3. Una vez se tiene el archivo protegido, se selecciona el modo de la aplicación de descifrado que recibe el archivo protegido, y la clave privada.

Condiciones del desarrollo

- La entrega debe ser un único proyecto en Netbeans en código Java.
- Debe escribir una clase llamada **FileShare** que contiene los métodos **crearClaves**, **cifrarArchivo** y **descifrarArchivo**.
- La clave pública se debe escribir en formato PEM.
- Utilice RSA de 1024 bits.
- La aplicación debe tener una interfaz gráfica simple, con las tres funciones: crear claves, cifrar archivo y descifrar archivo.
- Si utiliza código que ha sido escrito por otro, debe indicar claramente en el código las secciones del código tomadas, la URL de donde se toma, y el nombre del autor.
- Se pueden usar bibliotecas adicionales como BounceCastle.

Documentación

Escriba la documentación del proyecto utilizando JavaDoc y la guía de estilo de Google[3]. Genere un archivo PDF con la documentación de los métodos del proyecto.

Video de funcionalidad

Grabe un video de la funcionalidad de la aplicación. Desde el momento de la compilación y ejecución hasta el resultado final. La duración del video debe ser inferior a dos minutos. Debe cargar el video a Youtube y escribir el enlace en el manual de usuario.

Entrega

Cargue solo un (1) archivo comprimido en formato ZIP que contenga el proyecto, la documentación, y el manual de usuario, al Teams del curso. No cargue el video de funcionalidad a Teams, el video debe subirse a youtube.com. El plazo de entrega es el 13 de abril hasta las 23:59. Los grupos de trabajo se publican en el Teams del curso. La entrega se realiza en los grupos de trabajo, de dos estudiantes, definidos por el instructor.

Opcional

Calificación adicional para el grupo que implemente la capacidad de envío del archivo utilizado la red. Para la calificación y el video, se deben crear dos máquinas virtuales, cada una simula un usuario independiente. La aplicación además del archivo y la clave, permite ingresar la dirección IP del destinatario, enviar el archivo por la red. La aplicación destino, recibe el archivo y lo descifra con su clave privada.

---

[1] https://docs.oracle.com/javase/7/docs/technotes/guides/security/StandardNames.html
[2] https://docs.oracle.com/javase/7/docs/technotes/guides/security/certpath/CertPathProgGuide.html
[3] https://google.github.io/styleguide/javaguide.html

Evaluación

Puntos		0%	25%	75%	100%
12	Función creación de claves	No presenta la funcionalidad, o no compila el código	El código compila, pero no realiza ninguna de las tareas requeridas.	Crea las claves, pero no las almacena en el formato solicitado o no está en la GUI	Crea las claves, las almacena en el formato solicitado, y está asociada a la GUI.
12	Función cifrar archivo	No presenta la funcionalidad, o no compila el código.	El código compila, pero no realiza ninguna de las tareas requeridas.	Cifra el archivo con la clave pública, pero no está asociada a la GUI.	Cifra el archivo con la clave pública y está asociada a la GUI.
12	Función descifrar archivo	No presenta la funcionalidad, o no compila el código.	El código compila, pero no realiza ninguna de las tareas requeridas.	Descifra el archivo con la clave privada, pero no está asociada a la GUI.	Descifra el archivo con la clave privada y está asociada a la GUI.
8	Documentación del proyecto	No presenta documentación.	Presenta documentación simple pero no en el formato establecido.	Escribe documentación explicativa, cumple con la guía, pero no entrega el documento PDF.	La documentación es explicativa, sigue la guía de uso y entrega el documento en PDF.
6	Video manual	No presenta video.	El video explica una funcionalidad.	El video explica las tres funcionalidades, pero la duración es mayor a la indicada.	El video explica las tres funcionalidades de forma clara y la duración es la indicada.
10	Opcional. Envío de archivos entre dos aplicaciones por la red.	No presenta funcionalidad.			La aplicación permite el envío de archivos por la red.