PROTOCOLOS Y COMUNICACIONES SEGURAS

MEMORIA SOBRE LOS PROYECTOS REALIZADOS

Ciudad: SEGOVIA

Universidad: UNIVERSIDAD DE VALLADOLID

Campus: MARÍA ZAMBRANO

Centro: ESCUELA UNIVERSITARIA DE INFORMÁTICA

Identificación de la carrera: GRADO EN INGENIERÍA INFORMÁTICA DE SERVICIOS Y APLICACIONES

Asignatura: PROTOCOLOS Y COMUNICACIÓNES SEGURAS.

Número de Práctica: Memoria Final de Proyectos.

Nombres de los alumnos: IVÁN BARBADO, ABEL DE ANDRÉS y DIEGO MONJAS

D.N.I del alumno: 70262079 – T, 03475014 – J y 70260861 – R (Correspondientemente)

Fecha de Entrega: 22/01/2015

ESQUEMA DE TRABAJO

1. MOTIVACIÓN

Durante el curso 2014/2015 en el que se imparte la asignatura de Protocolos y Comunicaciones Seguras por el profesor José Ignacio Farrán, se reta a los alumnos a realizar una serie de proyectos en los que además de aprender y mejorar sus habilidades usando diferentes de programación se motiva a estos a utilizar el ingenio para conseguir realizar dichos proyectos.

2. OBJETIVOS

Los objetivos en dicha asignatura son realizar una serie de proyectos en los que se aplicaran los conocimientos obtenidos en las clases teóricas.

Los proyectos que a realizar son los siguientes:

- Cifrado Clásico. *Cesar* y *Vernam*.
- Método de Criptoanálisis. *Vigenère*.
- Cifrado en Flujo. *RC4*.
- Cifrado en Bloque en Varios Modos. *DES*.
- Funciones Hash. *SHA-1*.
- Método de Cifrado Público. *RSA*.
- Método de Firma Digital. *DSA*.
- Protocolo Criptográfico de Clave Pública de Aplicación Práctica. *Secreto Compartido de Shamir*.

El objetivo principal de la asignatura es entender cómo funciona cada algoritmo a desarrollar e implementarlo mediante un lenguaje de programación.

Obviamente es necesario que el alumno entienda como funciona cada algoritmo para poder implementarlo, de otra forma es muy complejo realizarlo.

3. ENTORNOS DE DESARROLLO Y LENGUAJES DE PROGRAMACION

Los entornos de desarrollo a utilizar son NetBeans IDE 8.0.1 y Maple.

Se ha decidido utilizar dichos entornos ya que facilitan el desarrollo del proyecto. Los lenguajes de programación a utilizar son Java y el lenguaje de programación de Maple.

Se han decidido utilizar dos entornos de desarrollo puesto que se podría decir que ambos lenguajes se complementan de alguna forma.

Por ejemplo, Maple facilita el desarrollo de los proyectos que son más numéricos, es decir cuenta con un entorno más matemático que Java. Por supuesto que Java tiene una gran cantidad de librerías de matemáticas para poder desarrollar los proyectos, pero Maple es bastante más visual.

También se ha utilizado Maple en el desarrollo de los proyectos de Java, ya que para hacer operaciones como la Exponenciación Modular que se utilizara frecuentemente se han tenido que utilizar librerías especiales y tipos de datos especiales en Java, mientras que en Maple no se exige dichas librerías o dichos tipos de datos. Por lo tanto es bastante más sencillo realizar las comprobaciones que con Java, que requiere además de utilizar métodos proporcionados por los datos y que a priori el alumno desconocía. Por ejemplo, para trabajar con números excesivamente grandes es necesario utilizar el tipo de dato BigInteger y utilizar sus propios métodos. En Maple esto no es necesario, aunque también tiene sus funciones.

Es necesario destacar que para desarrollar la mayoría de los proyectos se han utilizado arrays y listas para poder organizar los datos y operar con ellos, por lo tanto esta estructura de programación es de bastante ayuda y es necesario añadir que para los proyectos que utilicen esta estructura es mejor la programación en Java, por ejemplo en el proyecto de SHA-1, DES, Cesar, Vigenere, etc…

Por otro lado, generar las claves de cifrado y firmado resulta más sencillo utilizando Maple, ya que no es necesario utilizar tantas líneas de código como se utilizaría si lo implementásemos en Java. Del mismo modo ocurre con el Secreto Compartido de Shamir, en el que es necesario utilizar interpolación (en este caso interpolación polinómica de Lagrange). Realizar la interpolación resulta más sencillo en Maple ya que es un entorno totalmente matemático que proporciona mayor flexibilidad y ayuda que Java, aunque se podría haber realizado perfectamente en este lenguaje.

Cabe destacar que el algoritmo de Interpolación de Lagrange es conocido por el alumno ya que fue visto en la asignatura de Métodos Numéricos, por lo tanto nos ha servido de gran ayuda para realizar el proyecto del Secreto Compartido de Shamir.

4. NOTAS PARA EL DOCENTE

En cuanto al desarrollo de los proyectos de la asignatura han sido implementados por los 3 miembros del grupo, incluido los algoritmos de generación de claves de cifrado y firma y el algoritmo de cifrado, firma, descifrado y verificación de firma. Por consiguiente el grupo se responsabiliza de la funcionalidad de dichos algoritmos.

Por otro lado, cada miembro del grupo se responsabiliza individualmente del cifrado, firma, descifrado y verificación de firma de los mensajes enviados a sus compañeros y los recibidos por dichos compañeros.

5. CONCLUSIONES

Como dijimos anteriormente, esta asignatura ha llevado a los alumnos a aprender y mejorar sus habilidades en estos entornos de desarrollo (aprendiendo métodos nuevos, funciones, etc...) así como entender cómo se envía la información de forma segura para que otras personas no puedan obtener dicha información sin consentimiento o, aunque puedan obtener la información, no pueda ni comprenderla ni alterarla.

Nos ha resultado de gran interés puesto que hoy en día son muchas las personas y organizaciones que utilizan Internet para comunicarse y obviamente es necesario que estas comunicaciones se realicen de la forma más segura posible.