PRÁCTICA 3

CIFRADO ASIMÉTRICO Y FIRMA DIGITAL

En esta práctica vamos a implementar los sistemas de cifrado asimétrico más usuales. Como para ellos es necesario trabajar con números primos, implementaremos también un test de primalidad.

La práctica entonces se divide en tres partes:

3.1. Test de Miller-Rabin.

Dado un número impar p, hay que determinar si ese número es o no primo por medio del test de Miller-Rabin. Notemos que el test de Miller-Rabin no nos da la certeza de que un número sea primo, sino que eso lo hace con una cierta probabilidad que podemos hacer tan próxima a 1 como queramos, sin más que aplicar el test el número necesario de veces.

Los parámetros de entrada serán entonces un número impar p (el número que queremos comprobar si es o no primo), y un número natural m (el número de rondas máximo que aplicaremos el test). Y la respuesta debe ser: *El número p no es primo*, o *El número p es primo con probabilidad mayor que xxx* dependiendo de si pasa o no el test.

En cada ronda del test, hay que elegir un número al azar (diferente cada vez). Podemos elegir que el programa genere esos números aleatorios, o que se los introduzcamos directamente.

3.2. Cifrado asimétrico.

Aquí hay que implementar un sistema de cifrado asimétrico. Hay que elegir entre RSA, ElGamal, o curvas elípticas.

En este caso, el programa debe realizar tres tareas: generación de claves, cifrado y descifrado.

En la generación de claves, debe devolver dos ficheros de texto, uno con la clave pública y otro con la clave privada. Los distintos parámetros de las claves, aparecerán en líneas diferentes.

Para cifrar, se le introducirá el mensaje a cifrar y la clave pública (esta última a través de un fichero con el mismo formato que el generado en el apartado anterior).

Para descifrar, se le introducirá el mensaje cifrado y la clave privada, a través de un fichero con el mismo formato que el generado en el apartado primero.

3.3. Firma digital.

En esta sección se pide implementar un sistema de firma digital y verificación de la firma. Se puede elegir entre firma RSA, DSS o curvas elípticas.

Al igual que antes, debe realizar tres tareas: generación de claves, generación de firma y verificación de firma.

En la generación de claves, vale lo dicho en el apartado anterior.

Para la generación de la firma, se le introducirá un mensaje a cifrar (fichero) y el fichero con la clave (privada), y deberá generar una firma, que se guardará en un fichero de texto.

Puesto que lo que realmente se firma no es el mensaje, sino un resumen del mensaje, hay que generar un resumen de dicho mensaje. Para esto emplearemos la función SHA1 (se pueden añadir otras funciones resumen). Cualquiera de las implementaciones de esta función que hay en la red puede ser usada.

Para la verificación de la firma, se introduce el mensaje (fichero) que se ha firmado, un fichero con la firma (con el mismo formato que el generado en el apartado anterior) y un fichero con la clave (pública). Deberá responder si la firma es o no válida.

La fecha para la entrega es el día 4 de junio. Los ficheros hay que subirlos al SWAD, a la zona de ”Mis trabajos”. Si la práctica se hace en grupo, es suficiente con que la suba uno del grupo. Pero hay que indicar quienes son los componentes.

Para que la práctica se evalúe debe ser defendida por todos los miembros del grupo.