# Criptografía

## Práctica 3: Criptosistema RSA

ULPGC 2011-2012

*Implementación del algoritmo RSA para la encriptación de texto, en una aplicación Android para dispositivos móviles*

Gabriel Fernández Díaz
David Morales Sáez

## 1. Introducción

Para el desarrollo de esta práctica, se ha implementado el clásico algoritmo de encriptación RSA. Para ello hemos usado la tecnología Android, y por consiguiente, JAVA.

Además, se ha implementado una función para la generación de claves públicas y privadas, tanto usando números primos aleatorios como introducidos manualmente.

## 2. Trasfondo Teórico

El algoritmo RSA es un sistema de encriptación con clave pública, desarrollado en 1977 por Rivest, Shamir y Adleman.

El principio básico del algoritmo es la factorización de números enteros. Los mensajes son encriptados en formas de números y las claves usadas son dos números primos de gran tamaño. Una de las claves será pública y otra privada, esto se debe a que cada usuario tendrá una clave solo para si mismo, la privada, y otra que podrá saber todo el mundo, la pública. Esto se debe a que un mensaje encriptado con una clave solo puede ser desencriptada por su pareja, por lo que cuando un usuario desee ponerse en contacto con otro simplemente deberá encriptar el mensaje con la clave publica del destinatario, y solo este ultimo podrá leerlo. También puede ser usado como sistema de certificado digital. El usuario que desee certificar que un texto ha sido emitido, solo tiene que codificarlo con su clave privada, así todo el que desee comprobar la veracidad del documento solo deberá desencriptarlo con la clave pública y comprobar que el texto es coherente.

La fortaleza de este sistema se basa en que actualmente no hay ninguna forma de factorizar números primo con un coste en tiempo polinómico, por lo que no es viable intentar averiguar la clave privada usando la pública. Aunque en teoría es posible hacerlo usando algoritmos de superparalelización cuántica, aunque aún no ha sido posible implementarlos, o eso creemos.

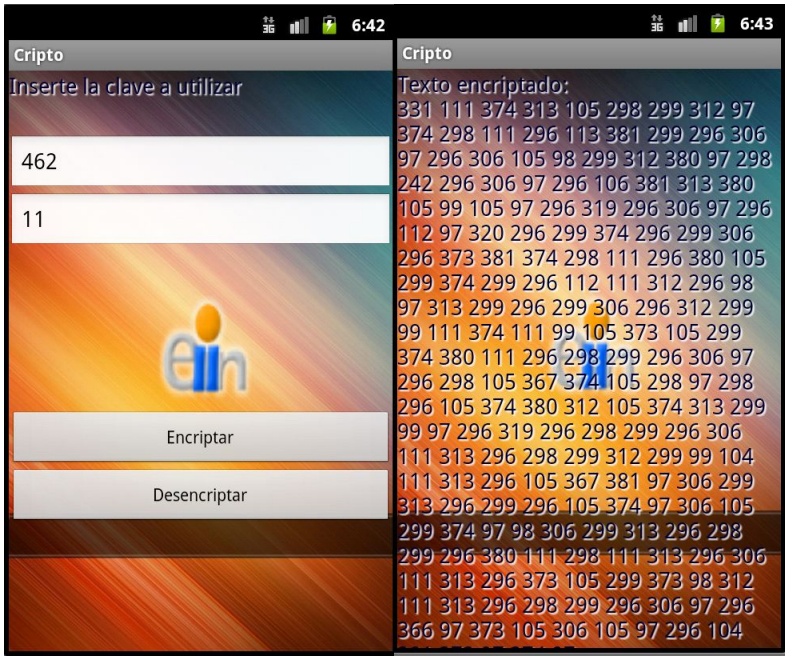
## 3. Implementación

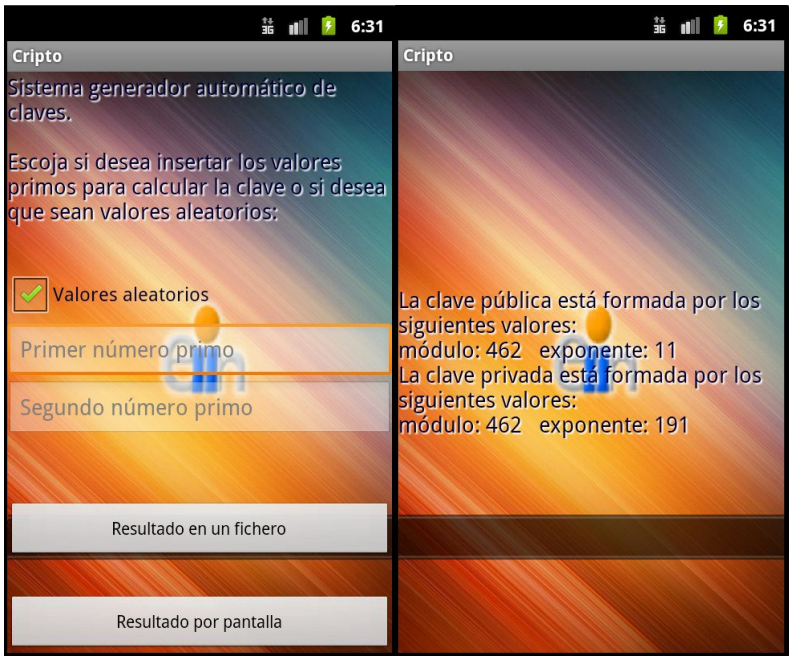
Para la implementación de esta práctica se ha añadido a la aplicación desarrollada para las prácticas anteriores las opciones de generar las claves y para codificar o descodificar usando el RSA.

## 4. Uso del programa

Para el correcto uso de la aplicación el proceso de uso es el siguiente:

1. Apretar el botón “RSA”
2. Seleccionar como insertar el texto
    a. Apretar “Inserte el Texto” para introducir el texto por pantalla, y luego presionar “Continue”
    b. Apretar “Escoja el Archivo” para introducir el texto desde un fichero, seleccionar el fichero origen y pulsar “Seleccionar”.
3. Seleccionar como mostrar el texto resultante
    a. Apretar “Resultado por pantalla” para mostrar el texto por pantalla.
    b. Apretar “Resultado en un fichero” para que el texto se guarde en un fichero, seleccionar el fichero destino y pulsar “Seleccionar”.
4. Introducir el modulo y el exponente de la clave deseada.
5. Pulsar “Encriptar” o “Desencriptar” según se deseé.


6:42
Cripto
Inserte la clave a utilizar
462
11
Encriptar
Desencriptar
6:43
Cripto
Texto encriptado:
331 111 374 313 105 298 299 312 97
374 298 111 296 113 381 299 296 306
97 296 306 105 98 299 312 380 97 298
242 296 306 97 296 106 381 313 380
105 99 105 97 296 319 296 306 97 296
112 97 320 296 299 374 296 299 306
296 373 381 374 298 111 296 380 105
299 374 299 296 112 111 312 296 98
97 313 299 296 299 306 296 312 299
99 111 374 111 99 105 373 105 299
374 380 111 296 298 299 296 306 97
296 298 105 367 374 105 298 97 298
296 105 374 380 312 105 374 313 299
99 97 296 319 296 298 299 296 306
111 313 296 298 299 312 299 99 104
111 313 296 105 367 381 97 306 299
313 296 299 296 105 374 97 306 105
299 374 97 98 306 299 313 296 298
299 296 380 111 298 111 313 296 306
111 313 296 373 105 299 373 98 312
111 313 296 298 299 296 306 97 296
366 97 373 105 306 105 97 296 104


6:31
Cripto
Sistema generador automático de claves.
Escoja si desea insertar los valores primos para calcular la clave o si desea que sean valores aleatorios:
Valores aleatorios
Primer número primo
Segundo número primo
Resultado en un fichero
Resultado por pantalla
6:31
Cripto
La clave pública está formada por los siguientes valores:
módulo: 462 exponente: 11
La clave privada está formada por los siguientes valores:
módulo: 462 exponente: 191