Seguridad de Sistemas Informáticos - práctica 5

Criptografía asimétrica

1. Generar un par de claves RSA de 4 cifras decimales.
   (a) Elegir dos números primos de dos cifras decimales p y q.
   (b) Calcular $n = p.q$ y $n' = (p-1)(q-1)$
   (c) Elegir el entero privado d, mayor que n' y coprimo con el mismo.
   (d) Buscar el entero público e tal que $e.d \bmod n' = 1$
   (e) La clave pública es (e,n) y la clave privada es (d,n)
2. Cifrar un número de 4 cifras decimales m menor que n utilizando la clave pública de un compañero. (se recomienda utilizar el comando bc). $c = m^e \bmod n$
3. Entregar c al compañero para que lo descifre con su correspondiente clave privada y recupere m. (otra vez utilizar el comando bc). $m = c^d \bmod n$. Comprobar que m esté correctamente calculado.
4. Utilizando el software gpg, generar un par de claves RSA-RSA de 3072 bits.

   ```
   gpg --full-gen-key
   ```

5. Exportar la clave pública a un archivo.

   ```
   gpg --armour --export <clave> --output <archivo>
   ```

6. Intercambiar los archivos de clave pública, e importar los archivos de clave pública de los compañeros.

   ```
   gpg --import <archivo>
   ```

7. Intercambiar mensajes cifrados.

   ```
   gpg -e -r <destinatario> ... --armour --output <archivo>
   ```

8. Descifrar los mensajes, utilizando las claves secretas.