CRYPT4YOU

DOCUMENTO ANEXO A LA LECCIÓN 1

DEL CURSO "EL ALGORITMO RSA"

EJERCICIOS Y PRÁCTICAS PROPUESTOS Y RESUELTOS

Autor: Dr. Jorge Ramió Aguirre
Fecha de publicación: 15 de marzo de 2012
Fecha de actualización: 26 de marzo de 2012
http://www.criptored.upm.es/crypt4you/temas/RSA/leccion1/leccion01.html

TABLA DE CONTENIDOS

LECCIÓN 1. LOS PRINCIPIOS DEL ALGORITMO RSA

Apartado 1.2. La seguridad del algoritmo RSA

ejercicioRSA1.2.1

Hagamos una sencilla prueba que nos permita comprender este tipo de problema.

Si te propongo que multipliques estos primos de uno, dos, tres y cuatro dígitos, no te será muy complicado hacer esos cálculos. Eso sí, deberías usar papel y lápiz, no una calculadora:

2 x 5 = _____; 31 x 53 = _____; 401 x 599 = _____; 3.911 x 8.009 = _____

Encontrarás que los productos son:

2 x 5 = 10; 31 x 53 = 1.643; 401 x 599 = 240.199; 3.911 x 8.009 = 31.323.199.

En los dos últimos casos has tenido que trabajar bastante más porque la entrada ha aumentado de tamaño.

Sin embargo, ahora te pido que encuentres -otra vez sin calculadora- cuáles son los dos primos que dan como producto los siguientes números compuestos de dos, cuatro, seis y ocho dígitos:

21 = p x q = ____; 2.183 = p x q = ____; 245.809 = p x q = ____; 1.379.087 = p x q= ____

verás que no lo tienes tan fácil ya en el segundo número porque lo primero que se nos ocurre es hacer la Criba de Eratóstenes (ver enlace), preguntando si el número es divisible por 2, 3, 5, 7, 11, ...etc., y eso conlleva una gran cantidad de operaciones, y obviamente también tiempo.

Web: http://amigosdelamatematica.blogspot.es/1202842500/

Con un poco de paciencia, y en el último caso muchísimo tiempo, encontraríamos que se trata de los productos entre los primos inmediatamente superiores a los que se usaron en la multiplicación previa. Es decir:

21 = 3 x 7 2.183 = 37 x 59 245.809 = 409 x 601 31.379.087 = 3.917 x 8.011

Podemos comprobar estos valores buscando en Google una tabla con los 10.000 primeros primos en la siguiente dirección.

Web: http://mimosa.pntic.mec.es/jgomez53/matema/conocer/10000_primos.htm

Obviamente existen algoritmos de factorización mucho mejores y eficientes que éste, pero no corresponde tratarlos aquí.

prácticaRSA1.2.1

Descarga el software factor.exe desde la zona de descarga de software básico de criptografía en Criptored e instálalo preferentemente en una carpeta que se llame C:\Criptolab\Factor. Este programa funciona desde MS-DOS en modo comando, por lo que debes ejecutarlo desde esa ventana del sistema, no haciendo doble clic en el icono.

SW factor: http://www.criptored.upm.es/paginas/software.htm#freeware

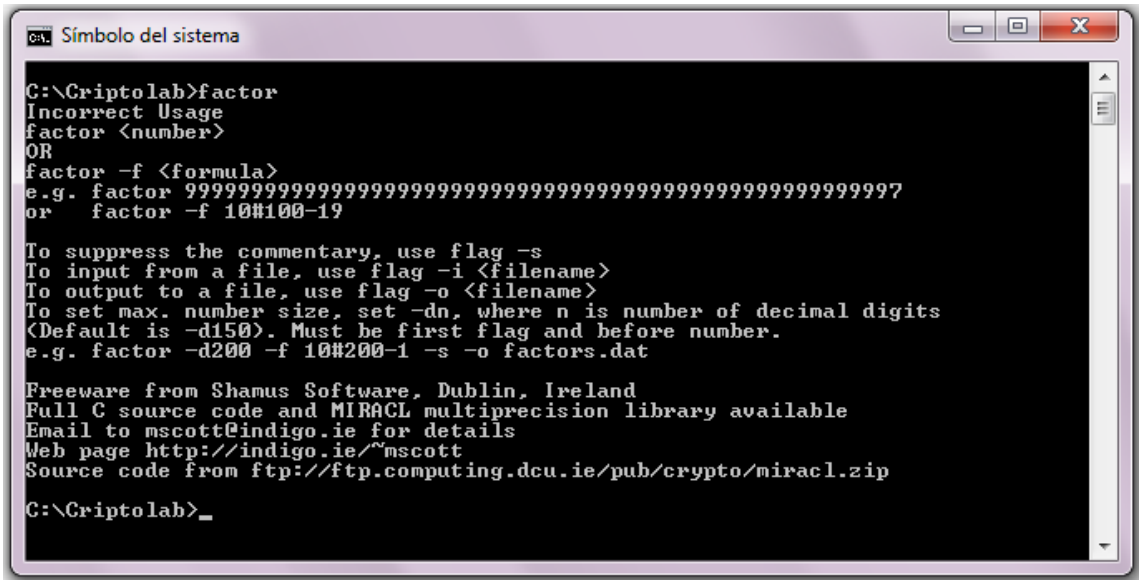
Encuentra los factores p y q de los siguientes números compuestos de 20, 30, 40, 50 y 60 dígitos, y observa cómo aumenta el tiempo de cálculo a medida que la entrada es mayor.

- Valor: 33133186298394380609
- Valor: 353468949918651760076444331007
- Valor: 49394653932702382117923122188025390462 21
- Valor: 44157175210767964375159342048568776952709498262057
- Valor: 18602185652665439895675839226649059604999885185980516444123 9

Haz una gráfica del tiempo empleado por el programa en factorizar esos números en función del número de dígitos de la entrada. Saca luego conclusiones.

Ayuda: usa la opción copiar y pegar el número usando el botón derecho del ratón, no Ctrl V.

En el último caso, debería tardar menos de un minuto.



Menú de Ayuda del programa factor.exe ante el comando factor (Enter)

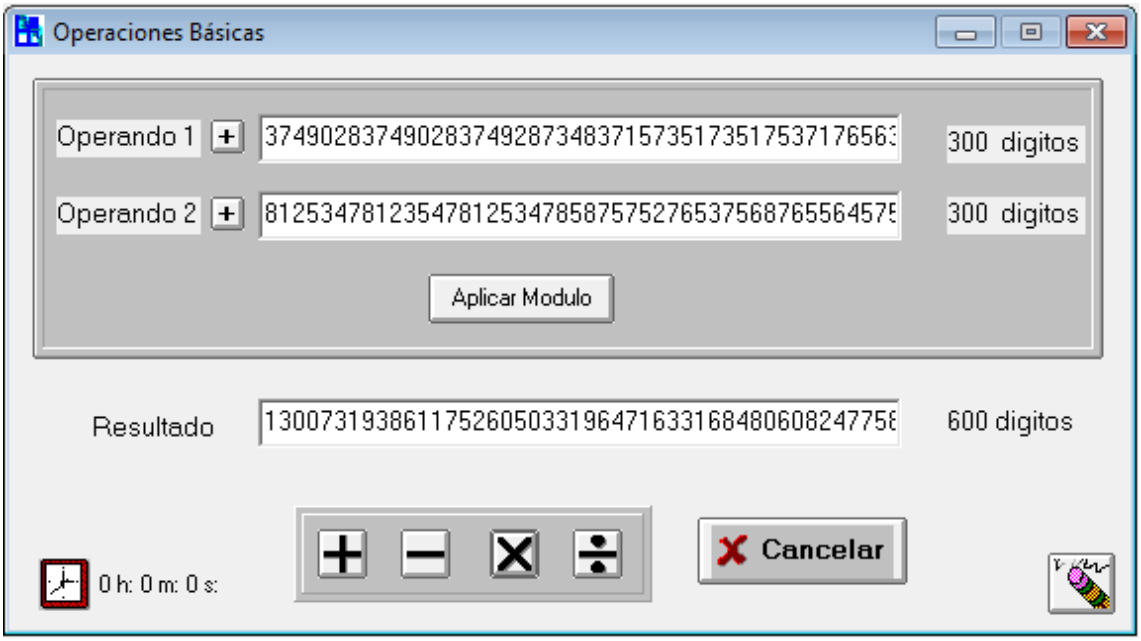
prácticaRSA1.2.2

Usa ahora el software Fortaleza de Cifrados para comprobar que, en cambio, la multiplicación de números grandes tiene un comportamiento polinomial y además es muy rápido. Descarga el software e instálalo en la carpeta Criptolab, es decir, C:\Criptolab\Fortaleza.

SW Fortaleza de Cifrados: http://www.criptored.upm.es/software/sw_m001e.htm

1. Ejecuta el programa Fortaleza y en la barra de iconos pulsa en las dos herramientas, arriba a la izquierda.
2. Elige la operación Op_Basic de Operaciones Básicas.
3. Introduce (copia y pega) los siguientes valores de Op1 y Op2 de 40, 80 y 120 dígitos y calcula su producto.
4. Al final, multiplica dos números aleatorios de 300 dígitos cada uno, lo máximo que acepta este software.
5. Observa lo que tarda el programa en dar el resultado de la multiplicación en cada caso.

- Op1 = 98712365276465465468514654256527657978 22
- Op2 = 98642376562865464651654276507 6174654276
- Op1 = 54543465465465176592786027656341765081109101897826622255129815672442354355523451
- Op2 = 56457534976572747626546854276527576452765976527648762576545265465426971118768820
- Op1 = 56352356476767627646542797680726765765278597625765761765276783472597052956497625563176517459767463417658078973568017646 5
- Op2 = 98974577357656154277625625766245361707620655423467766208752564367657961346298926525734532124336529843265287572908765622 7



Tiempo del producto de dos números de 300 dígitos (app. 1.000 bits cada uno)

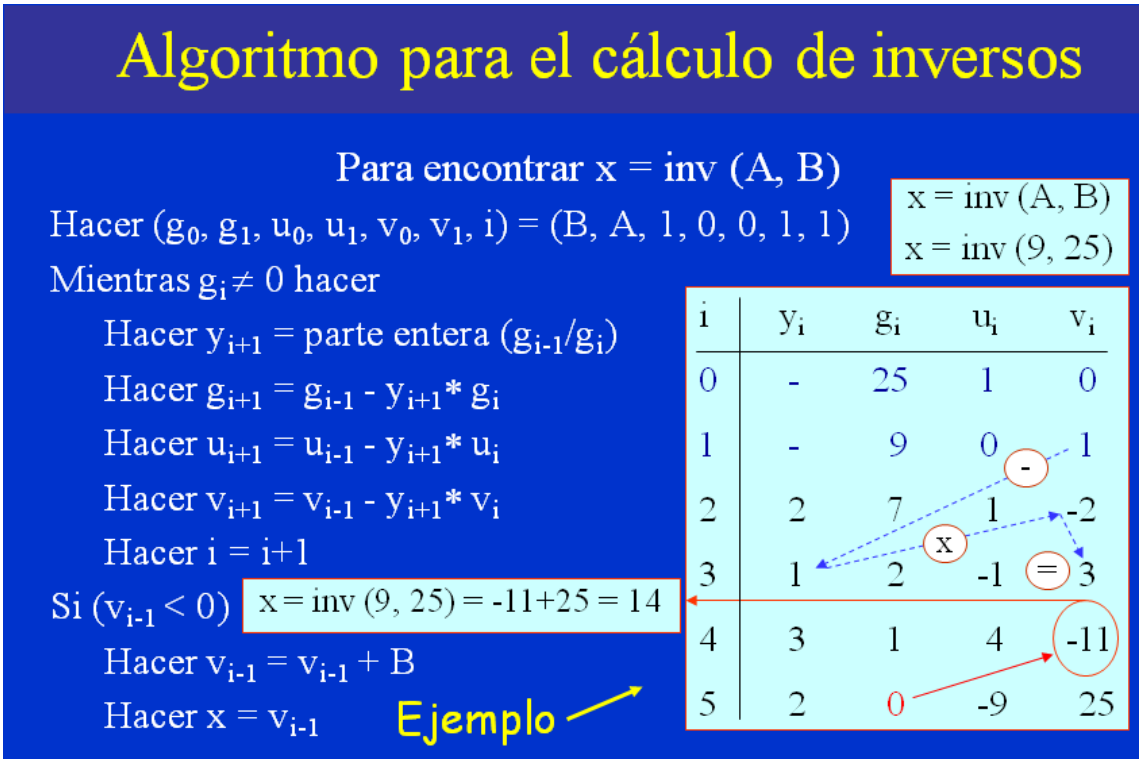
Apartado 1.3. Esquema de generación de claves con dos usuarios Alicia y Bernardo

ejercicioRSA1.3.1

Busca en esta tabla de primos el primer primo mayor que el número 50 y el último primo menor que el número 100 para obtener, en cada caso, el primo p y el primo q.

Web: http://mimosa.pntic.mec.es/jgomez53/matema/conocer/10000_primos.htm

1. Calcula el cuerpo de trabajo n y el Indicador de Euler ϕ (n).
2. Elige como clave pública e el primer número válido mayor que 20.
3. Usa el algoritmo extendido de Euclides para encontrar la clave privada d. Puedes ver en la siguiente figura cómo se ejecuta este algoritmo.
4. No uses ningún programa para calcular este inverso.
5. Comprueba con una calculadora que el producto de la clave pública e por la clave privada d dentro del cuerpo ϕ (n) es igual a 1.



Ejemplo del Algoritmo Extendido de Euclides AEE para calcular d = inv [e, ϕ (n)]

ejercicioRSA1.3.2

Sin usar ningún programa, genera una clave RSA a partir de dos primos de 3 dígitos cada uno, y que además q sea aproximadamente el doble de p. Elige luego una clave pública e superior al número 30 y encuentra la clave privada d.

1. Buscamos esos dos primos, por ejemplo p = 461 y q = 919.
2. El cuerpo de trabajo será n = 461 x 919 = 423.659.
3. El Indicador de Euler ϕ (n) = (p - 1)(q - 1) será:
   ϕ (423.659) = (461 - 1)(919 - 1) = 460 x 918 = 422.280.
4. Buscaremos un número e para la clave pública, entre 3 y ϕ (n) - 2 que sea válido, es decir que cumpla mcd [e, ϕ (n)] = 1.
5. Elegimos un número cualquiera, por ejemplo superior a 30, que cumpla con esa condición. En este caso el 37 puesto que mcd (37, 422.280) = 1.
6. Calculamos mediante el algoritmo extendido de Euclides AEE la clave
   d = inv [e, ϕ (n)] = inv (37, 422.280) = 11.413.
7. Efectivamente, exd = 37x11.413 = 422.2781; se sale del cuerpo ϕ (n) sólo una vez.
8. Damos a conocer nuestra clave pública: n = 423.659; e = 37.
9. Guardamos en secreto nuestra clave privada: d = 11.413.

Puedes ver cómo funciona el AEE en el Capítulo 7 del Libro Electrónico de Seguridad Informática y Criptografía V 4.1

Web: http://www.criptored.upm.es/guiateoria/gt_m001a.htm

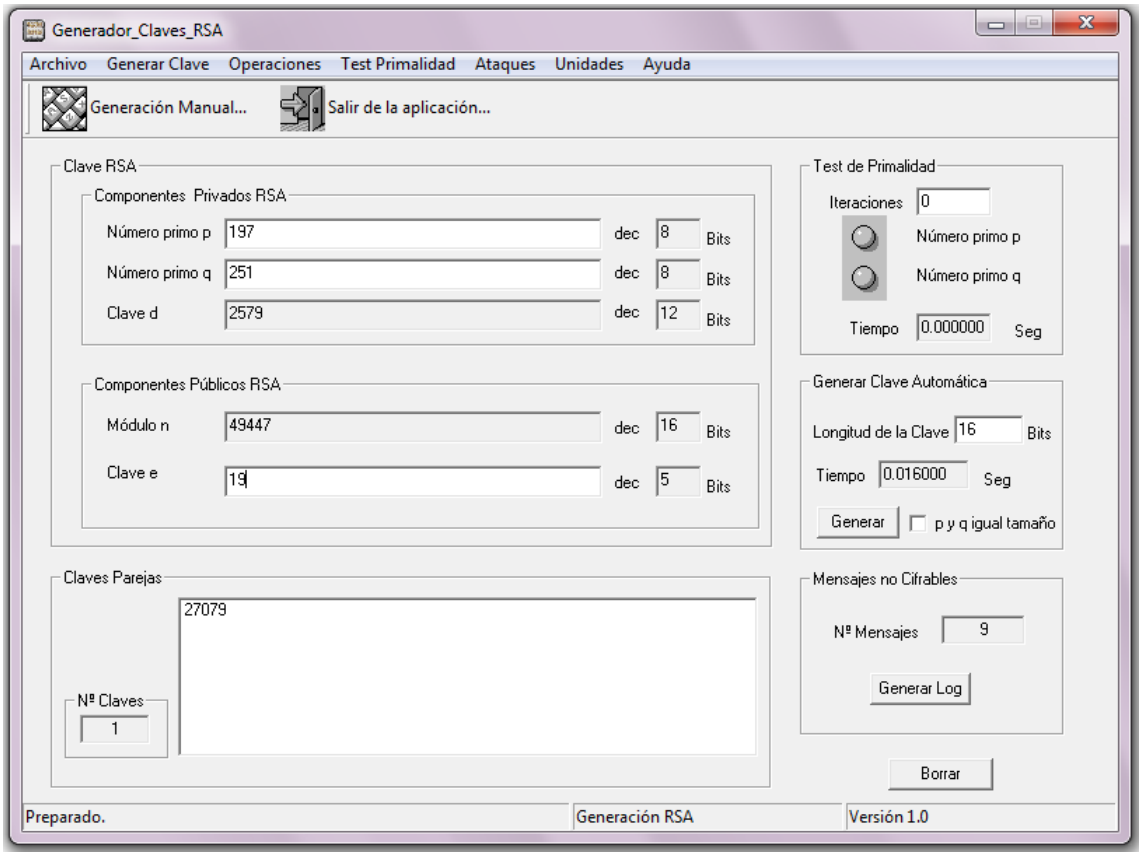
prácticaRSA1.3.1

Descarga el software genRSA e instálalo en la carpeta C:\Criptolab\genRSA.

SW genRSA: http://www.criptored.upm.es/software/sw_m001d.htm

Genera una clave RSA donde p = 197, q = 251, e = 19.

1. Ejecutamos el programa genRSA e introducimos estos valores en las casillas de p, q y e, usando la opción copiar y pegar.
2. Pegamos los valores 197, 251 y 19.
3. Desde la parte superior izquierda de la aplicación, pulsamos Generación Manual.
4. Obtenemos la clave que aparece en la siguiente figura, donde:
5. La clave pública es n = 49.447 y e = 19, siendo la clave privada d = 2.579.
6. No te preocupes de momento por las Claves Privadas Parejas y los Mensajes No Cifrables que muestra el programa genRSA en la parte inferior; se estudiarán en próximas lecciones.



Generación de la clave de la práctica con genRSA

prácticaRSA1.3.2

Usa el software genRSA y sigue estos pasos, genera las claves que se indican a continuación.

SW genRSA: http://www.criptored.upm.es/software/sw_m001d.htm

Paso 1:

1. Si ya estás trabajando en una sesión con genRSA, en la parte inferior derecha de la pantalla de la aplicación, pulsa Borrar.
2. En la zona Generar Clave Automática, pon como longitud de clave 24 bits.
3. Pulsa en esa zona de la pantalla el botón Generar.
4. Una vez vista la clave generada, vuelve a pulsar varias veces Generar y observa las claves generadas
5. Activa la opción p y q de igual tamaño y vuelve a generar algunas claves de forma automática.
6. Saca conclusiones de lo observado.

Paso 2:

1. Pulsa el botón Borrar para limpiar la pantalla de valores.
2. Desde el Menú pulsa en Unidades y elige Hexadecimal.
3. Introduce los siguientes valores para p, q y e con la opción copiar y pegar.
4. p = 3F44BBBF.
5. q = 39838831.
6. e = 5BD5.
7. Desde la parte superior derecha de la aplicación, pulsa Generación Manual.
8. Saca conclusiones de lo observado.

Paso 3:

1. Pulsa el botón Borrar para limpiar la pantalla de valores.
2. Genera claves automáticas como en el caso anterior para tamaños de 512 bits, 1.024 bits y 2.048 bits (en la aplicación no pongas puntos en los miles) tanto para p y q de igual tamaño como distintos.
3. Observa las claves generadas y saca conclusiones de lo observado.

Apartado 1.4. Operaciones de cifrado y descifrado RSA entre Alicia y Bernardo

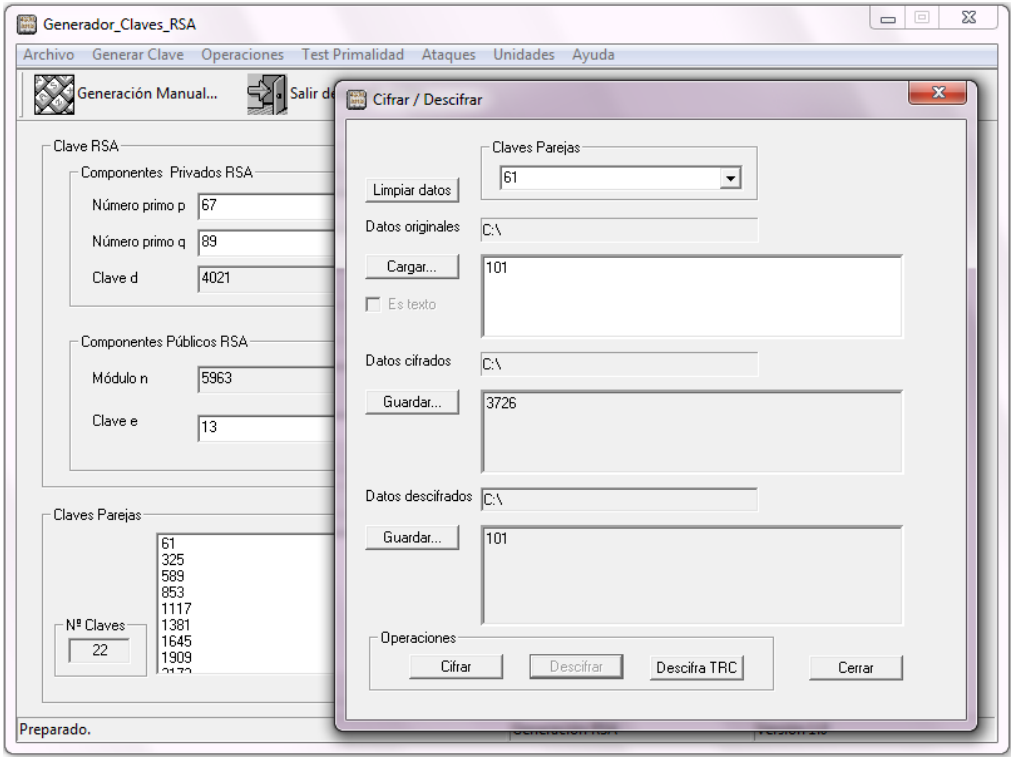
ejercicioRSA1.4.1

Alicia tiene como clave pública RSA los valores n_A = 5.963 y e_A = 13. Bernardo desea enviarle de forma confidencial el número secreto N = 101. Indica las operaciones de cifrado y descifrado y usa para comprobarlo el software genRSA.

SW genRSA: http://www.criptored.upm.es/software/sw_m001d.htm

1. Bernardo hace la siguiente operación N^{eA} mod $n_A = 101^{13}$ mod 5.963 = 3.726.
2. Como n = 5.963, es fácil comprobar que p_A = 67 y q_A = 89.
3. Por tanto ϕ (n_A) = 66 x 88 = 5.808 y d = inv (13, 5.808) = 4.021.
4. Puedes realizar este cálculo usando la calculadora de Windows.
5. Alicia recibe el criptograma C = 3.726 y realiza la operación C^{dA} mod n_A.
6. C^{dA} mod $n_A = 3.726^{4.021}$ mod 5.963 = 101.
7. Puedes realizar también este cálculo usando la calculadora de Windows.
8. Alicia recupera el valor secreto 101 enviado por Bernardo.

La siguiente figura muestra las operaciones de cifrado y descifrado con el programa genRSA. Recuerda que este programa sólo realiza la cifra usando la clave pública.



Captura de pantalla de la práctica

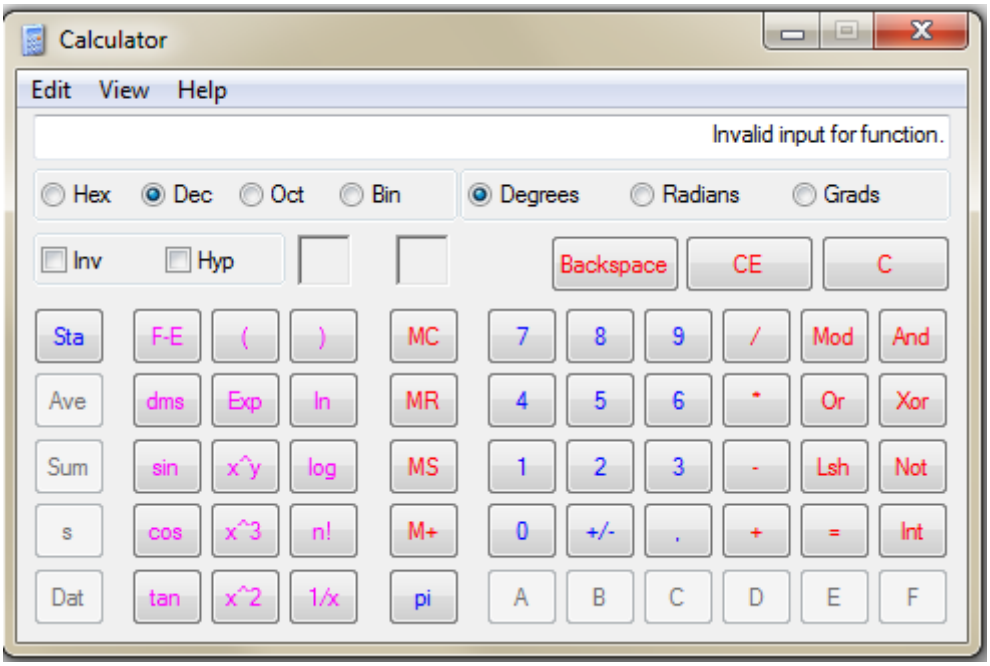
prácticaRSA1.4.1

Intenta realizar la siguiente operación con la calculadora de Windows:

$$100245^{30479} \bmod 790657667.$$

Los valores están indicados sin puntos para que puedas usar la opción de copiar y pegar.

Como puedes comprobar, se trata de una operación válida con una clave RSA válida, que debería entregar el resultado 74.948.040. Pero no hemos podido realizar dicha operación al obtener el mensaje de error "Invalid input for function" cuando pulsamos Mod.



Operación Mod no válida en calculadora de Windows para números grandes

1. Comprueba que el resultado de la operación es 74.948.040.
2. ¿Cuáles serían los primos p y q de esta clave RSA?
3. Si 30.479 es la clave pública e, ¿cuál es el valor de la clave privada d?
   Puedes usar el software que ya conoces.

prácticaRSA1.4.2

Usa el software genRSA para cifrar el siguiente mensaje.

SW genRSA: http://www.criptored.upm.es/software/sw_m001d.htm

1. Genera con genRSA manualmente una clave RSA con p = 3221, q = 3433, e = 31.
2. Generada la clave, pulsa en el Menú Operaciones Cifrar/Descifrar e introduce el valor 123, no texto.
3. Pulsa cifrar para obtener el criptograma.
4. Pulsa descifrar para recuperar el número secreto.
5. Comprueba este resultado con el software Fortaleza de Cifrados y con la calculadora de Windows.

prácticaRSA1.4.3

Usa el software genRSA y genera estas claves en hexadecimal.

SW genRSA: http://www.criptored.upm.es/software/sw_m001d.htm

1. Con genRSA cambia las unidades a hexadecimal. Si tienes datos en la pantalla borra esa clave (abajo a la derecha) y luego cambia de unidades.
2. Genera de forma automática una clave de 1024 bits con los primos p y q de igual tamaño.
3. Generada la clave, cambia el valor de clave pública e por el siguiente valor.
4. e = 010001.
5. Pulsa en el icono Generación Manual.
6. ¿Al cambiar la clave pública e, qué cosas cambian en la clave?
7. ¿Qué tipo de clave "interesante" crees que has generado en esta sencilla práctica?

Apartado 1.5. Operaciones de firma y comprobación de firma RSA entre Alicia y Bernardo

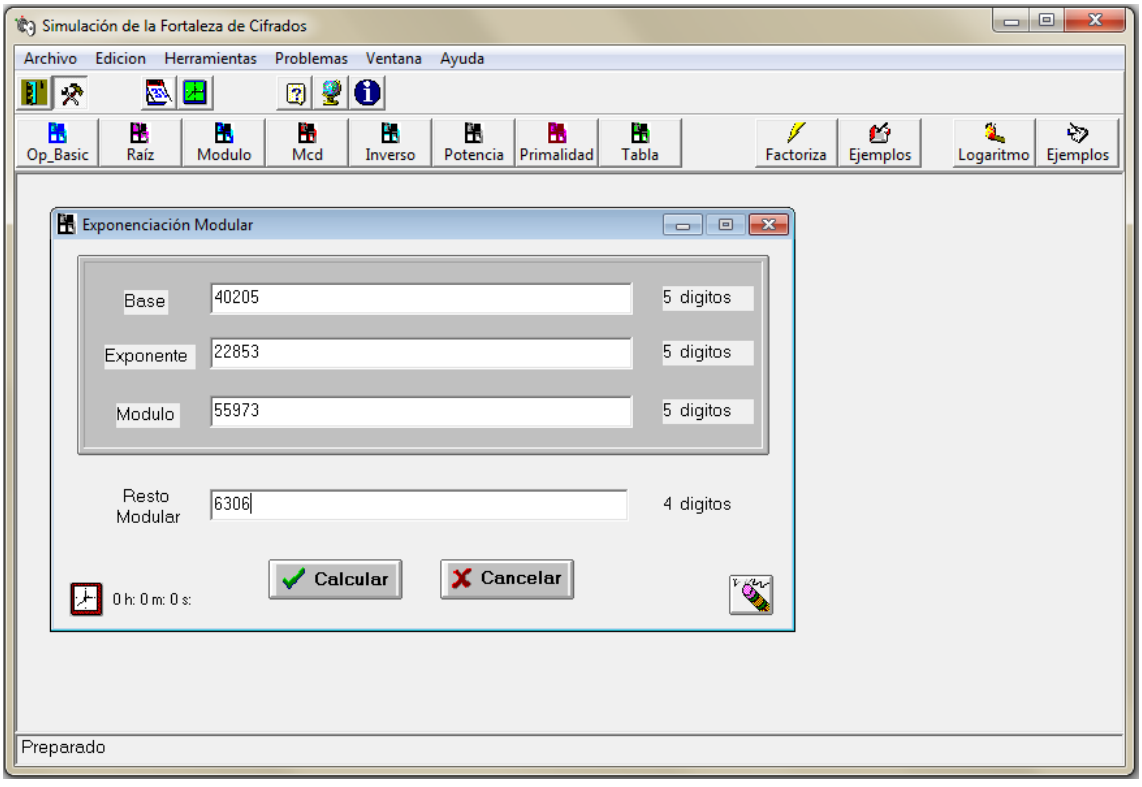
prácticaRSA1.5.1

Bernardo desea enviarle a Alicia firmado el valor 40.205. La clave pública de Bernardo es n_B = 55.973 y e_B = 17, y su clave privada d_B = 22.853.

Puesto que $M^d = 40.205^{22.853} \bmod 55.973$ resulta un número grande para la calculadora de Windows, usamos Fortaleza de Cifrados.

SW Fortaleza de Cifrados: http://www.criptored.upm.es/software/sw_m001e.htm

1. Ejecutamos el programa Fortaleza y en la barra de iconos pulsamos en las dos herramientas, arriba a la izquierda.
2. Elegimos la operación potencia.
3. Introducimos los valores 40205, 22853 y 55973.
4. Obtenemos como resultado de firma el valor 6306.
5. Con el mismo software, usando ahora la clave pública de Bernardo e = 17, comprobamos que el valor firmado es 40.205.



Captura de pantalla de la práctica con software Fortaleza de Cifrados