

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:

$$2 \times 5 = \underline{\hspace{2cm}}; \quad 31 \times 53 = \underline{\hspace{2cm}}; \quad 401 \times 599 = \underline{\hspace{2cm}}; \quad 3.911 \times 8.009 = \underline{\hspace{2cm}}$$

Encontrarás que los productos son:

$$2 \times 5 = 10; \quad 31 \times 53 = 1.643; \quad 401 \times 599 = 240.199; \quad 3.911 \times 8.009 = 31.323.199..$$

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:

$$21 = p \times q = \underline{\hspace{2cm}}; \quad 2.183 = p \times q = \underline{\hspace{2cm}}; \quad 245.809 = p \times q = \underline{\hspace{2cm}}; \quad 1.379.087 = p \times q = \underline{\hspace{2cm}}$$

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.

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:

$$21 = 3 \times 7 \quad 2.183 = 37 \times 59 \quad 245.809 = 409 \times 601 \quad 1.379.087 = 3.917 \times 8.011$$

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

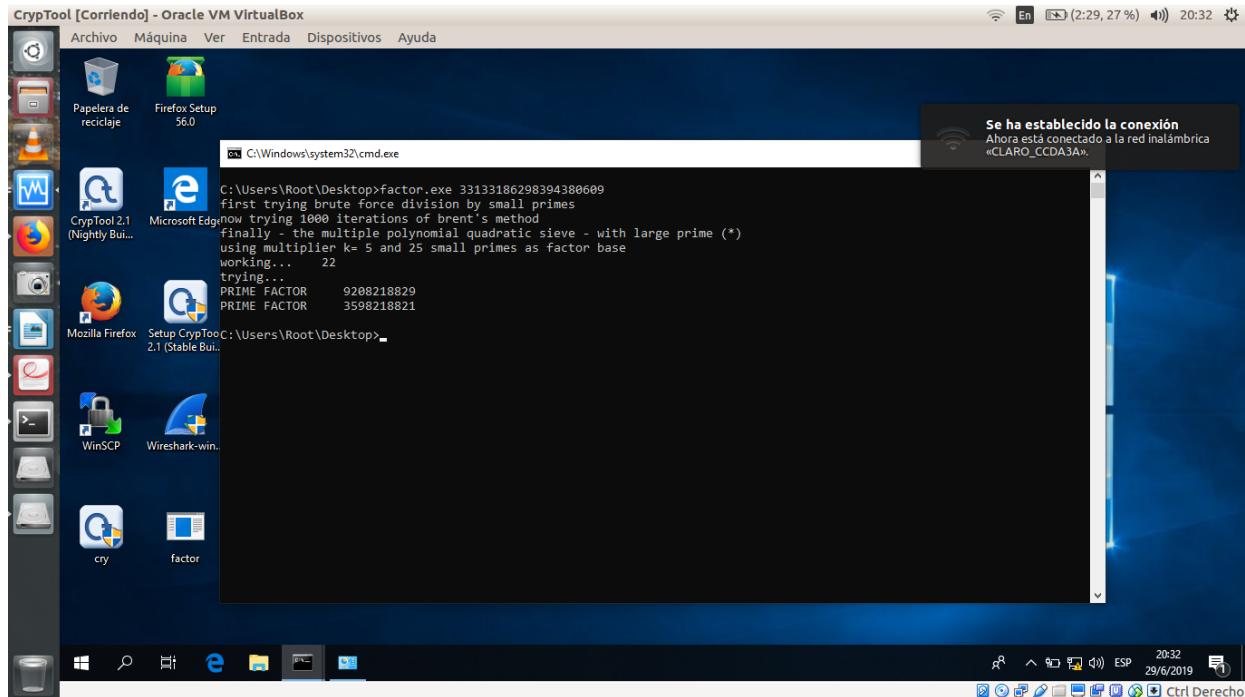
Obviamente existen algoritmos de factorización mucho mejores y eficientes que éste, pero no corresponde tratarlos aquí.

PrácticaRSA1.2.1

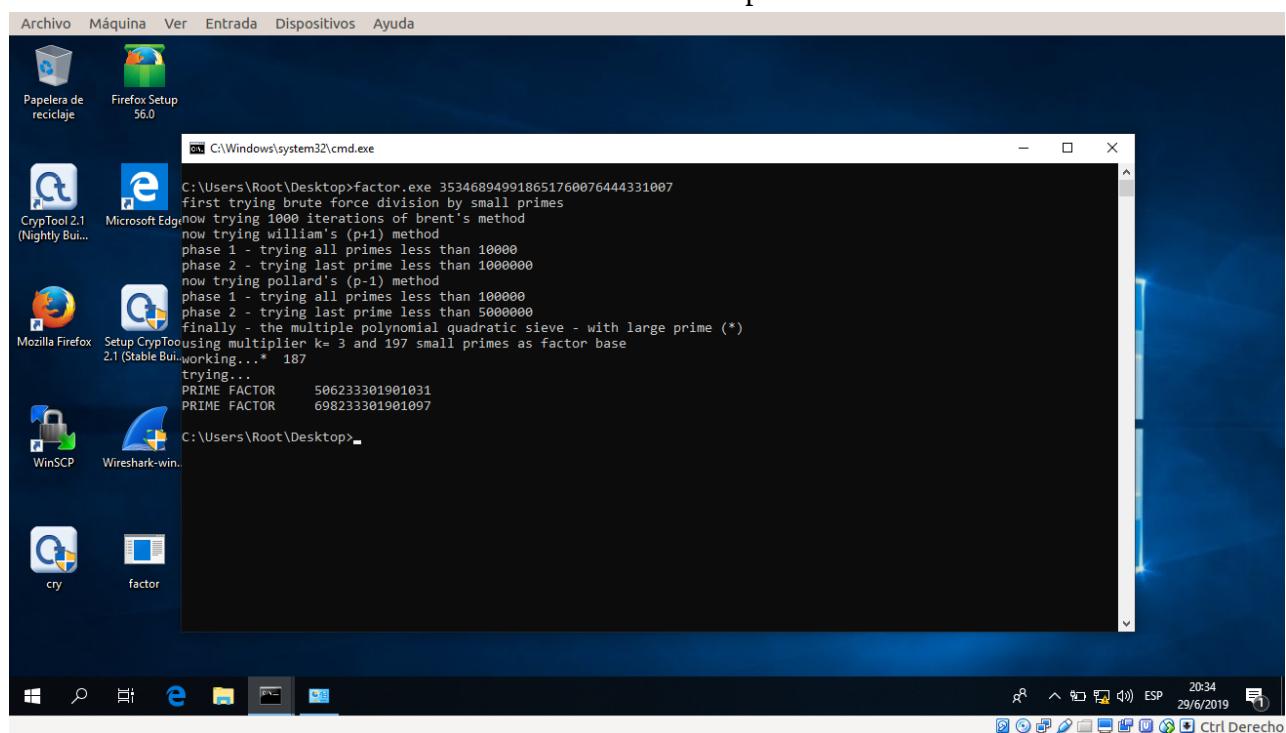
Descarga el software factor.exe desde la zona de descarga de software básico de criptografía en Criptored e instálalo preferentemente en una carpeta que se llame C:\Criptolab\Factor. Este programa funciona desde MS-DOS en modo comando, por lo que debes ejecutarlo desde esa ventana del sistema, no haciendo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

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.

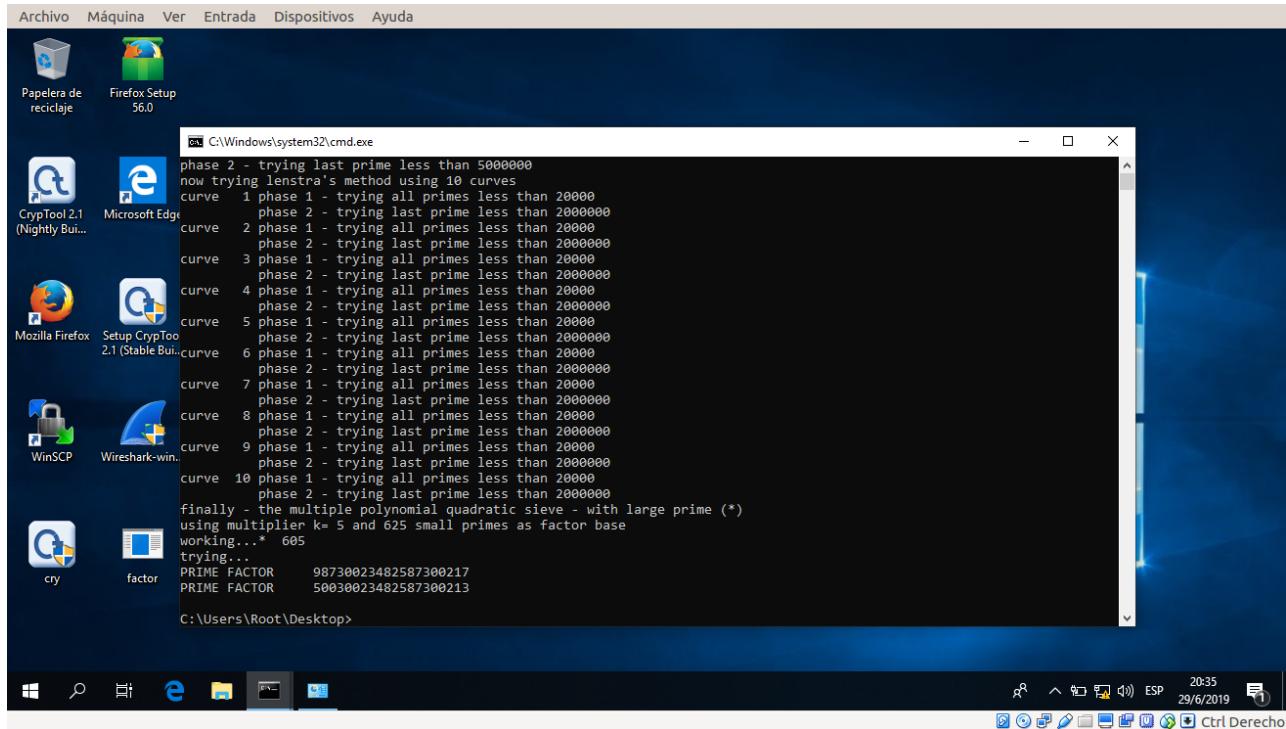
- Valor: 33133186298394380609 su tiempo fue 0.1s.



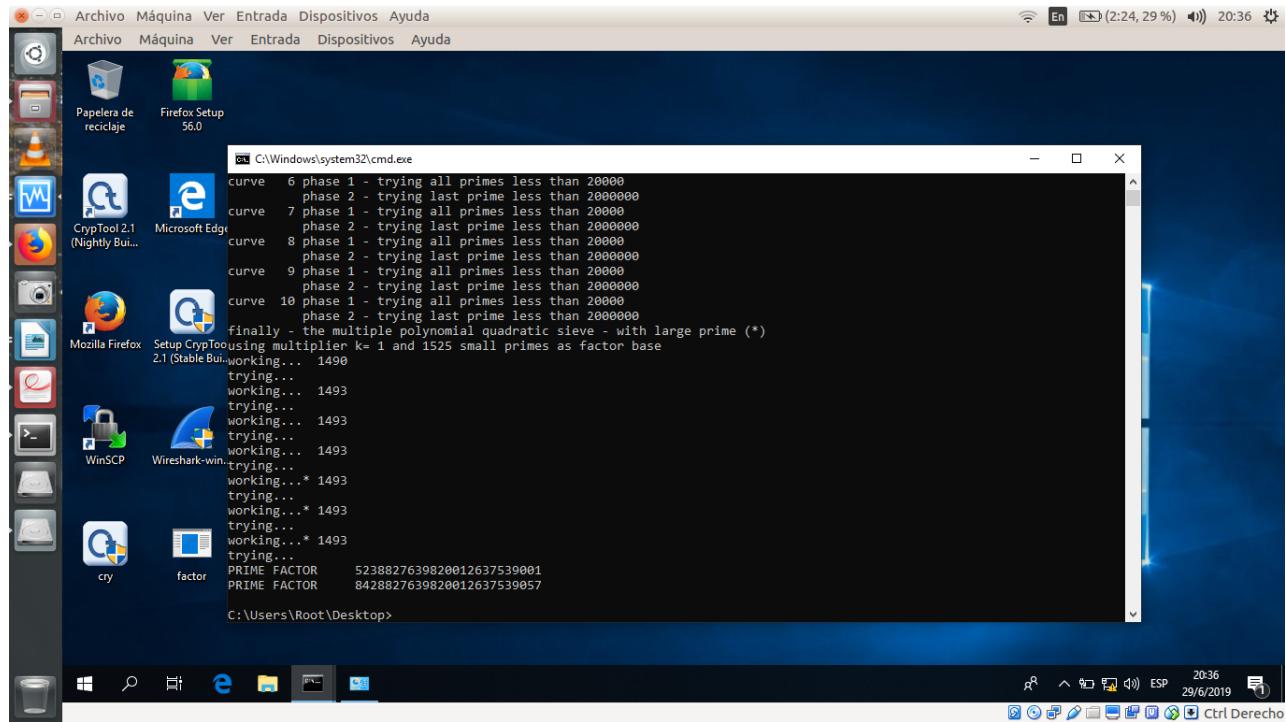
- Valor: 353468949918651760076444331007 su tiempo fue 0.5s



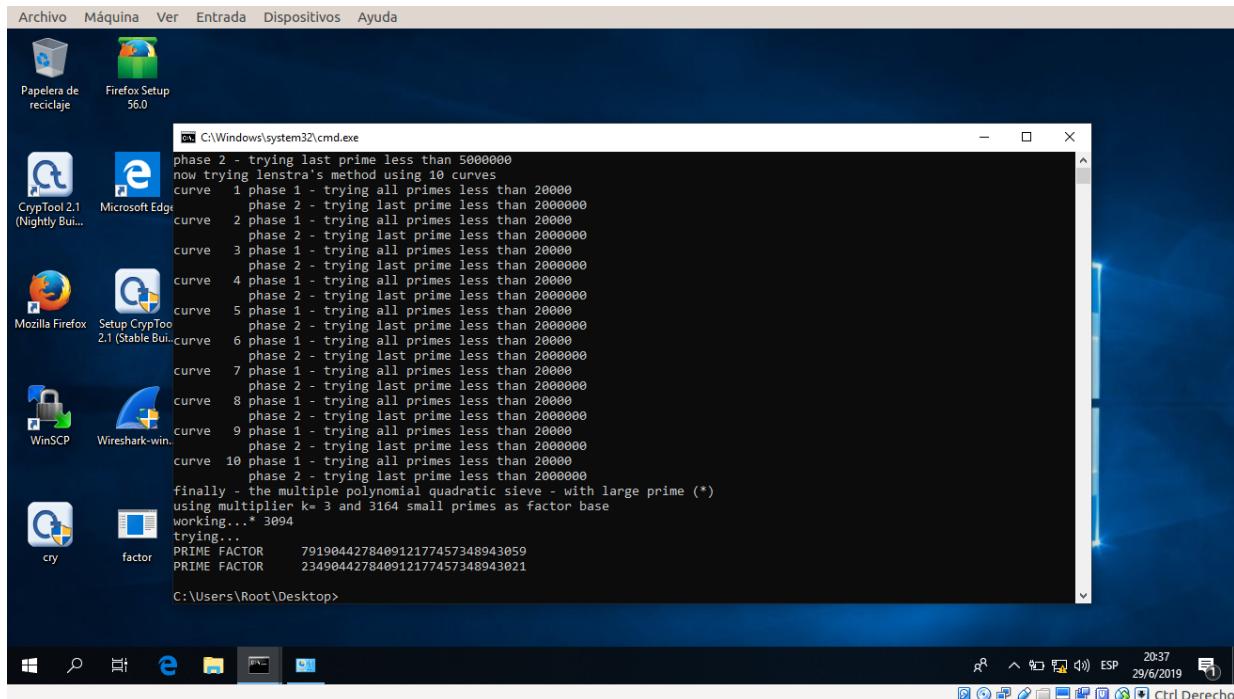
- Valor: 4939465393270238211792312218802539046221 su tiempo fue 1.90s



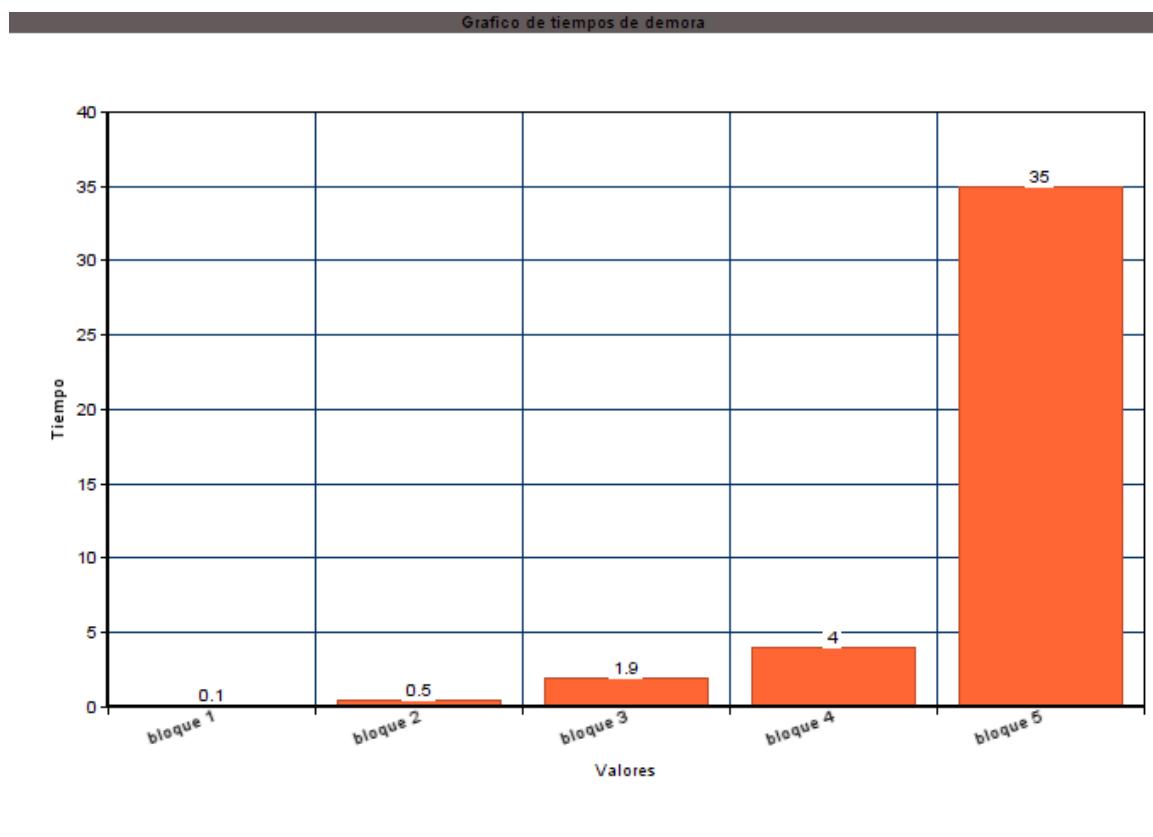
- Valor: 44157175210767964375159342048568776952709498262057 su tiempo fue 4s



- Valor: 186021856526654398956758392266490596049998851859805164441239 su tiempo fue 35s



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.



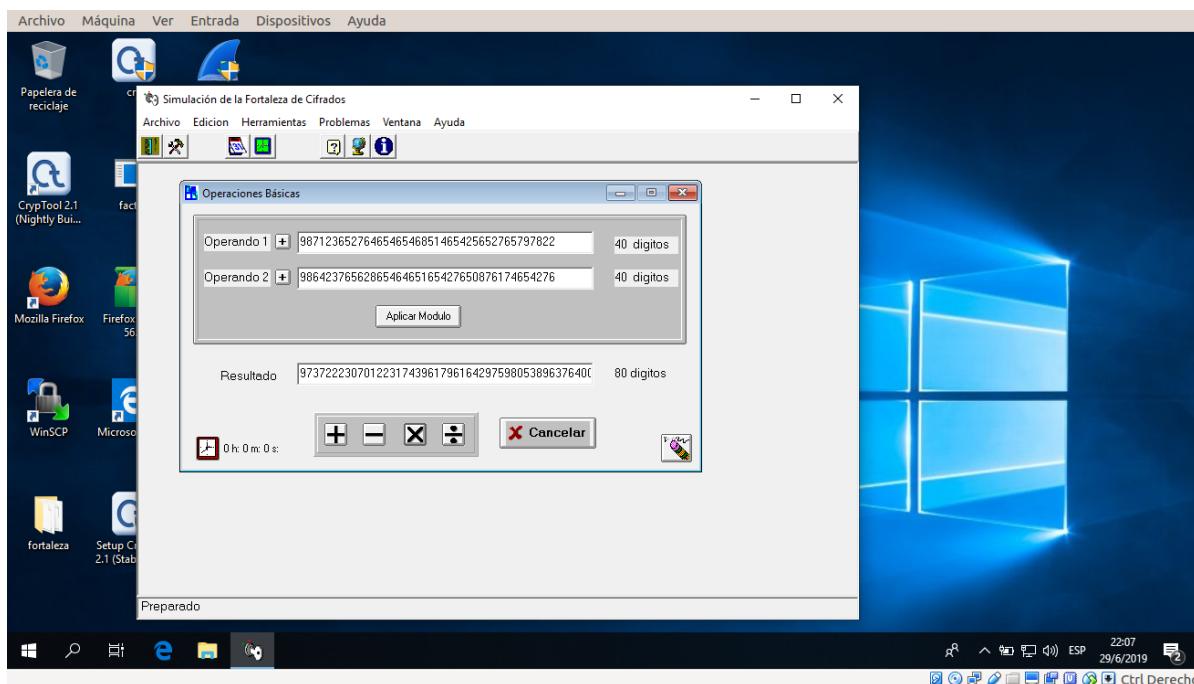
Ayuda: usa la opción copiar y pegar el número usando el botón derecho del ratón, no Ctrl V. En el último caso, debería tardar menos de un minuto.

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.

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 = 9871236527646546546851465425652765797822
 - Op2 = 9864237656286546465165427650876174654276

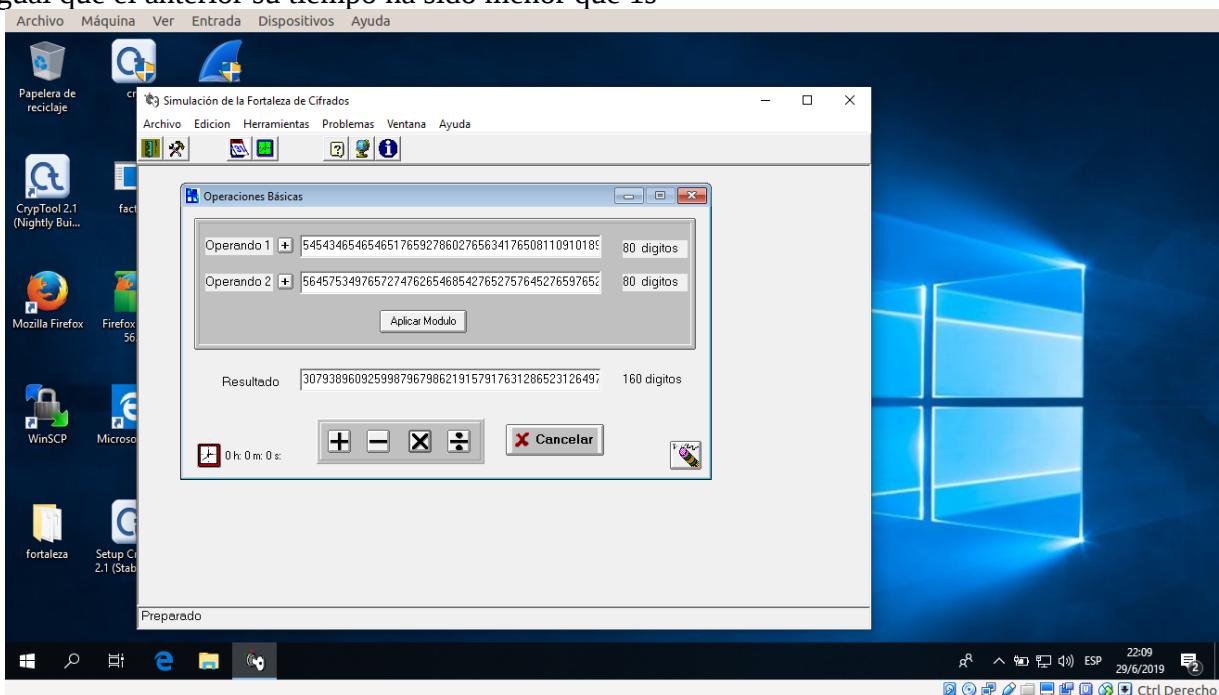
En esta operación se ha demorado menos de 1s



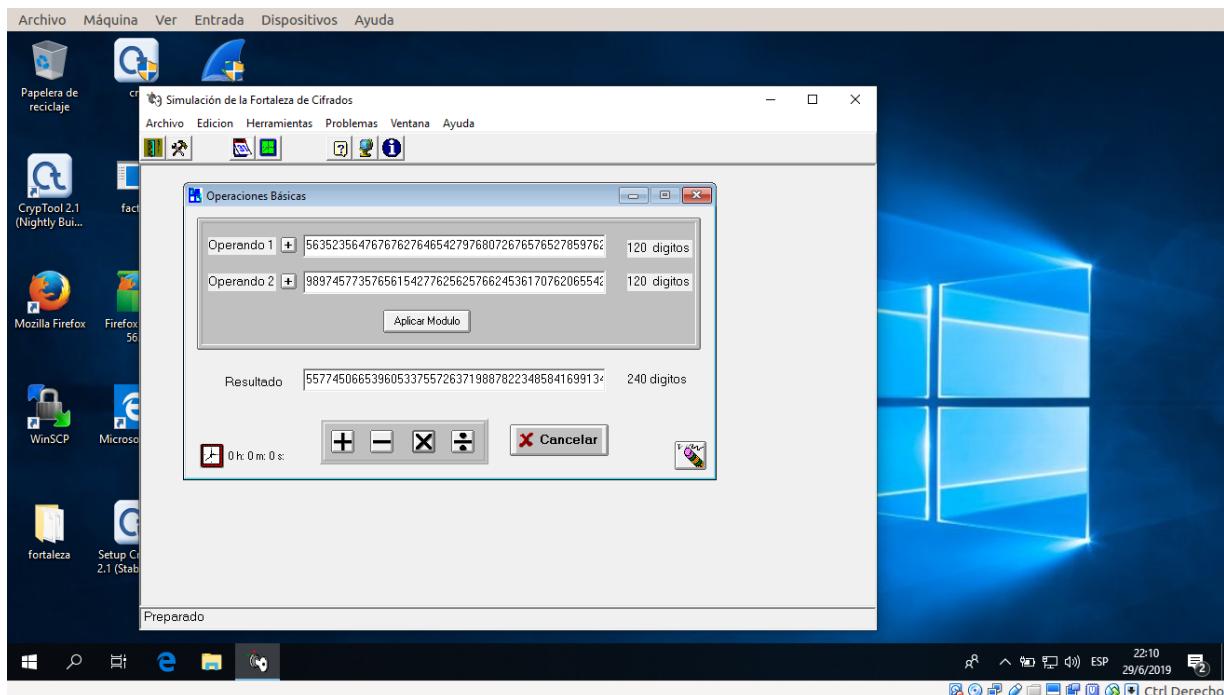
- Op1=545434654654651765927860276563417650811091018978266222551298156724423543
55523451

- $Op2=564575349765727476265468542765275764527659765276487625765452654654269711$
 18768820

Al igual que el anterior su tiempo ha sido menor que 1s

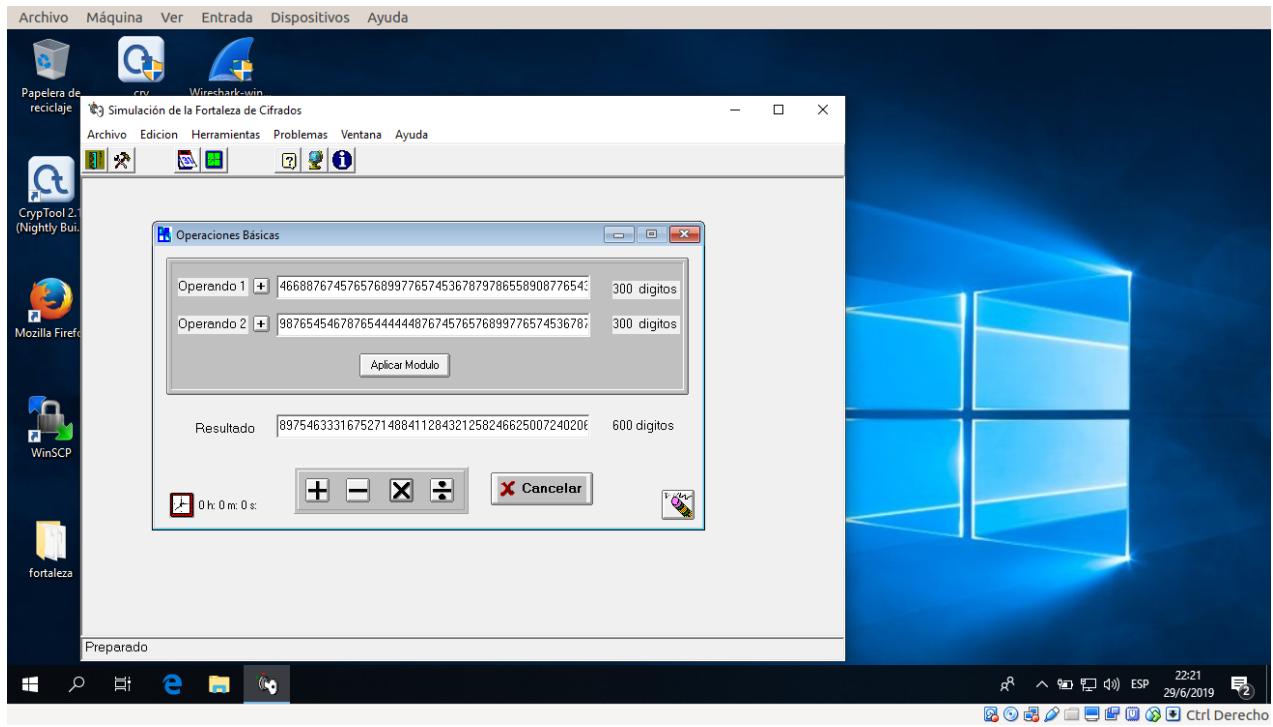


- $Op1=5635235647676276465427976807267657652785976257657617652767834725970529$
 $564976255631765174597674634176580789735680176465.$
- $Op2=989745773576561542776256257662453617076206554234677662087525643676579613$
 $462989265257345321243365298432652875729087656227$



Al igual que en los ejercicios pasados este apesar que no es notorio se demora un poco mas que los demás.

Números aleatorios de 300 dígitos cada uno, lo máximo que acepta este software.



En este ejercicio su demora ha sido calculada al menos de 1.5s.

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.

1. Calcula el cuerpo de trabajo n y el Indicador de Euler $\phi(n)$.

Dado que en la tabla el primero numero primo mayor que 50 es 53 y el primero numero menor que 100 es 97 podemos decir que:

El cuerpo de trabajo será $n = 53 \times 97 = 5141$

El Indicador de Euler $\phi(n) = (p - 1)(q - 1)$ será: $\phi(5141) = (53 - 1)(97 - 1) = 52 \times 96 = 4992$.

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.

Calculamos mediante el algoritmo extendido de Euclides la clave
 $d = \text{inv}[e, \phi(n)] = \text{inv}(23, 4992) = 217.0434$

Efectivamente, $exd = 23 \times 217.0434 = 4991.9982$

Damos a conocer nuestra clave pública: $n = 4992$; $e = 23$.
 Guardamos en secreto nuestra clave privada: $d = 217.0434$

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 $\phi(n)$ es igual a 1.

Algoritmo para el cálculo de inversos

Para encontrar $x = \text{inv}(A, B)$

Hacer $(g_0, g_1, u_0, u_1, v_0, v_1, i) = (B, A, 1, 0, 0, 1, 1)$

$$x = \text{inv}(A, B)$$

$$x = \text{inv}(9, 25)$$

Mientras $g_i \neq 0$ hacer

Hacer $y_{i+1} = \text{parte entera } (g_{i-1}/g_i)$

Hacer $g_{i+1} = g_{i-1} - y_{i+1} * g_i$

Hacer $u_{i+1} = u_{i-1} - y_{i+1} * u_i$

Hacer $v_{i+1} = v_{i-1} - y_{i+1} * v_i$

Hacer $i = i + 1$

Si ($v_{i-1} < 0$) $x = \text{inv}(9, 25) = -11 + 25 = 14$

Hacer $v_{i-1} = v_{i-1} + B$

Hacer $x = v_{i-1}$

Ejemplo

i	y_i	g_i	u_i	v_i
0	-	25	1	0
1	-	9	0	1
2	2	7	1	-2
3	1	2	-1	3
4	3	1	4	-11
5	2	0	-9	25

Ejemplo del Algoritmo Extendido de Euclides AEE para calcular $d = \text{inv}[e, \phi(n)]$

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 $n = 461 \times 919 = 423.659$.
3. El Indicador de Euler $\phi(n) = (p - 1)(q - 1)$ será: $\phi(423.659) = (461 - 1)(919 - 1) = 460 \times 918 = 422.280$.
4. Buscaremos un número e para la clave pública, entre 3 y $\phi(n) - 2$ que sea válido, es decir que cumpla $\text{mcd}[e, \phi(n)] = 1$.
5. Elegimos un número cualquiera, por ejemplo superior a 30, que cumpla con esa condición. En este caso el 37 puesto que $\text{mcd}(37, 422.280) = 1$.
6. Calculamos mediante el algoritmo extendido de Euclides AEE la clave $d = \text{inv}[e, \phi(n)] = \text{inv}(37, 422.280) = 11.413$.

7. Efectivamente, $exd = 37 \times 11.413 = 422.2781$; se sale del cuerpo $\varphi(n)$ sólo una vez.
8. Damos a conocer nuestra clave pública: $n = 423.659$; $e = 37$.
9. Guardamos en secreto nuestra clave privada: $d = 11.413$.

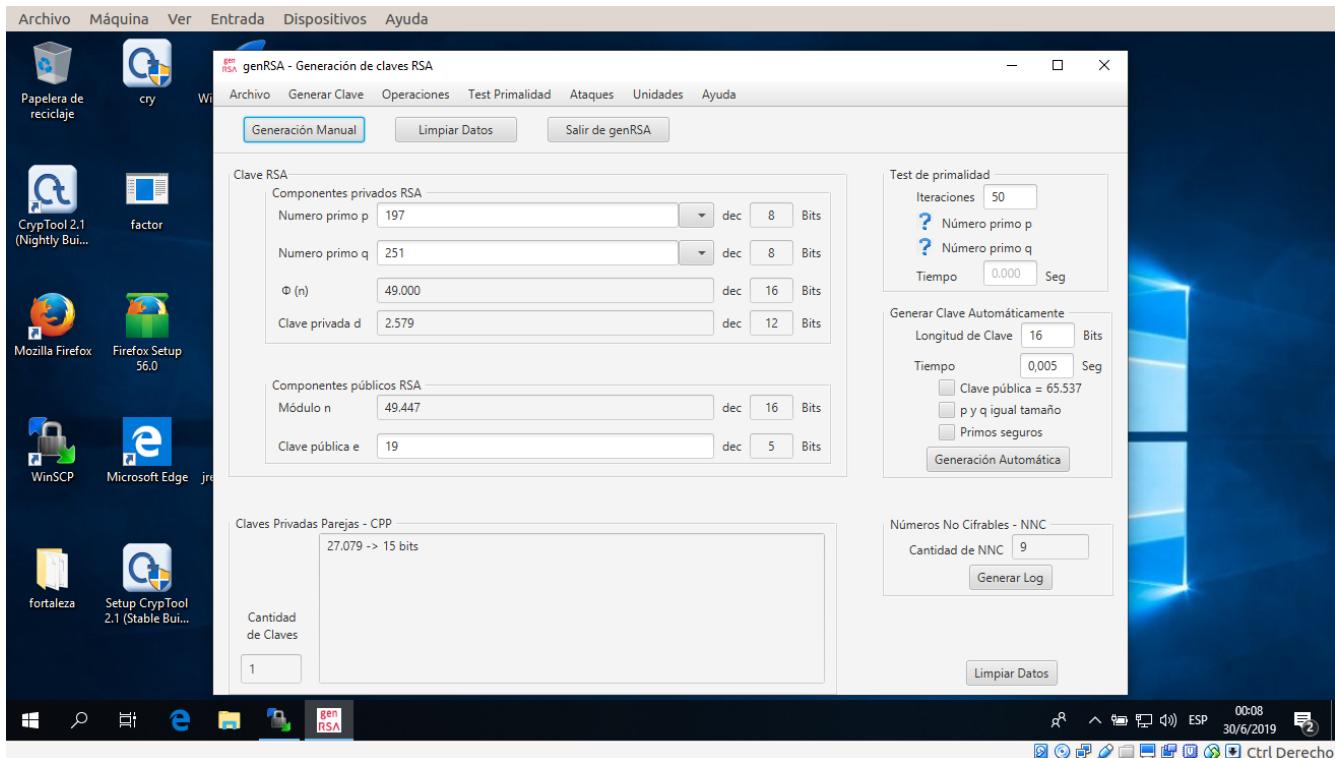
Puedes ver cómo funciona el AEE en el Capítulo 7 del Libro Electrónico de Seguridad Informática y Criptografía V 4.1

PrácticaRSA1.3.1

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

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.

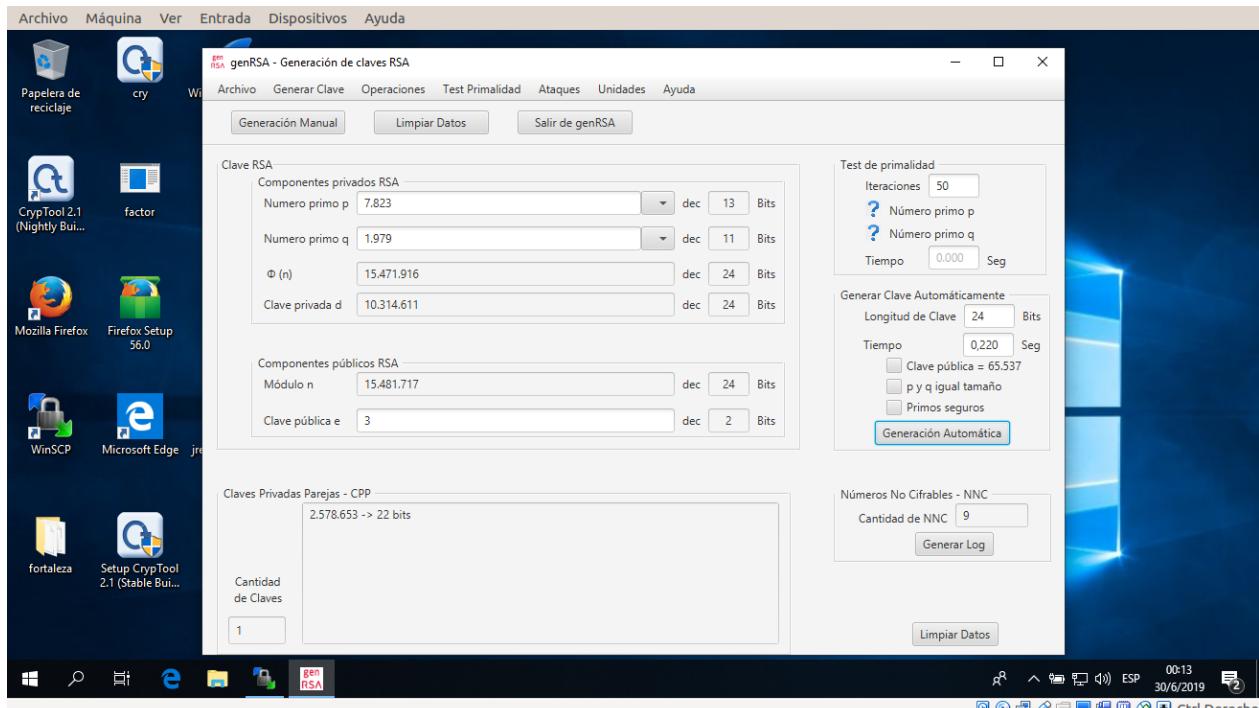


PrácticaRSA1.3.2

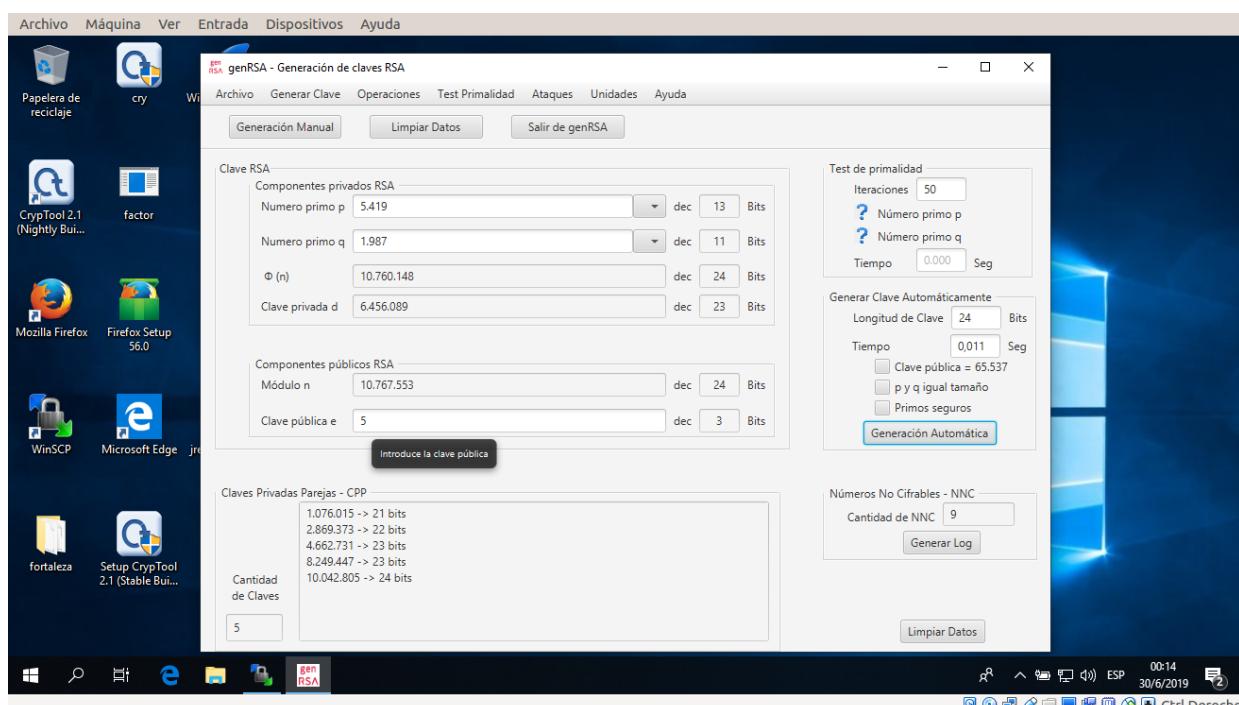
Usa el software genRSA y sigue estos pasos, genera las claves que se indican a continuación.

Paso 1:

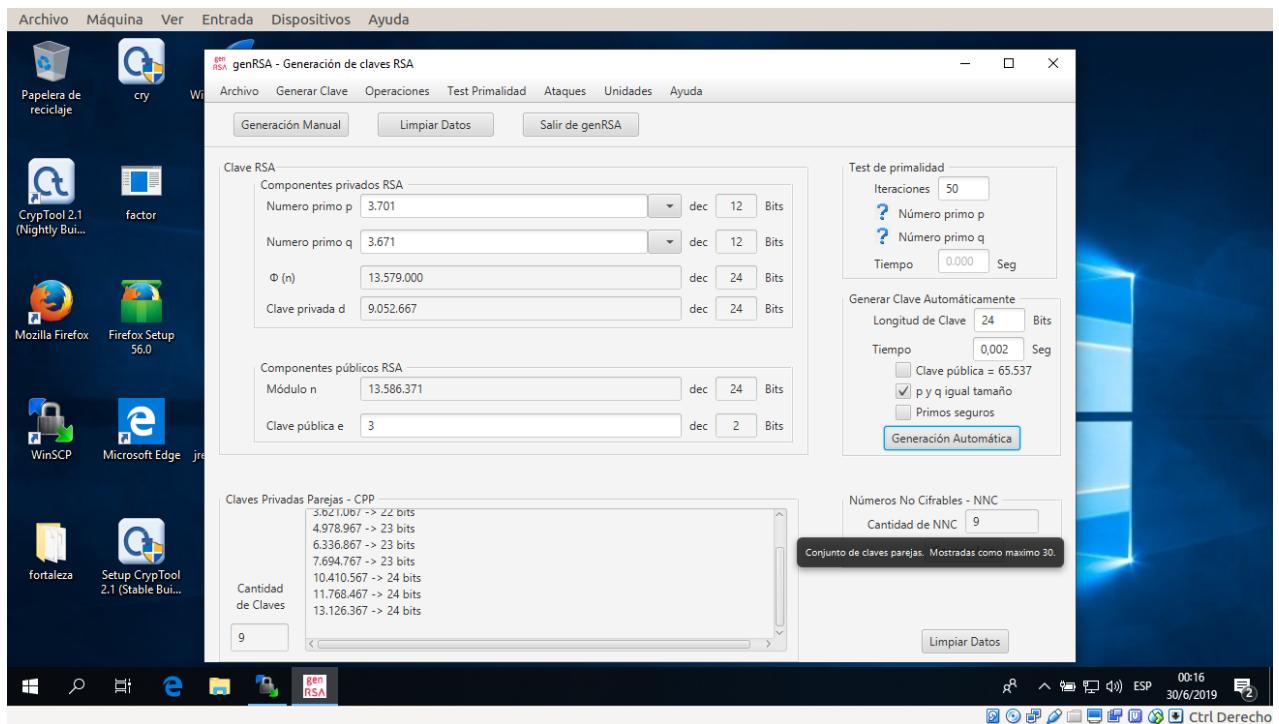
1. Si ya estás trabajando en una sesión con genRSA, en la parte inferior derecha de la pantalla de la aplicación, pulsa Borrar.
2. En la zona Generar Clave Automática, pon como longitud de clave 24 bits.
3. Pulsa en esa zona de la pantalla el botón Generar.



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.

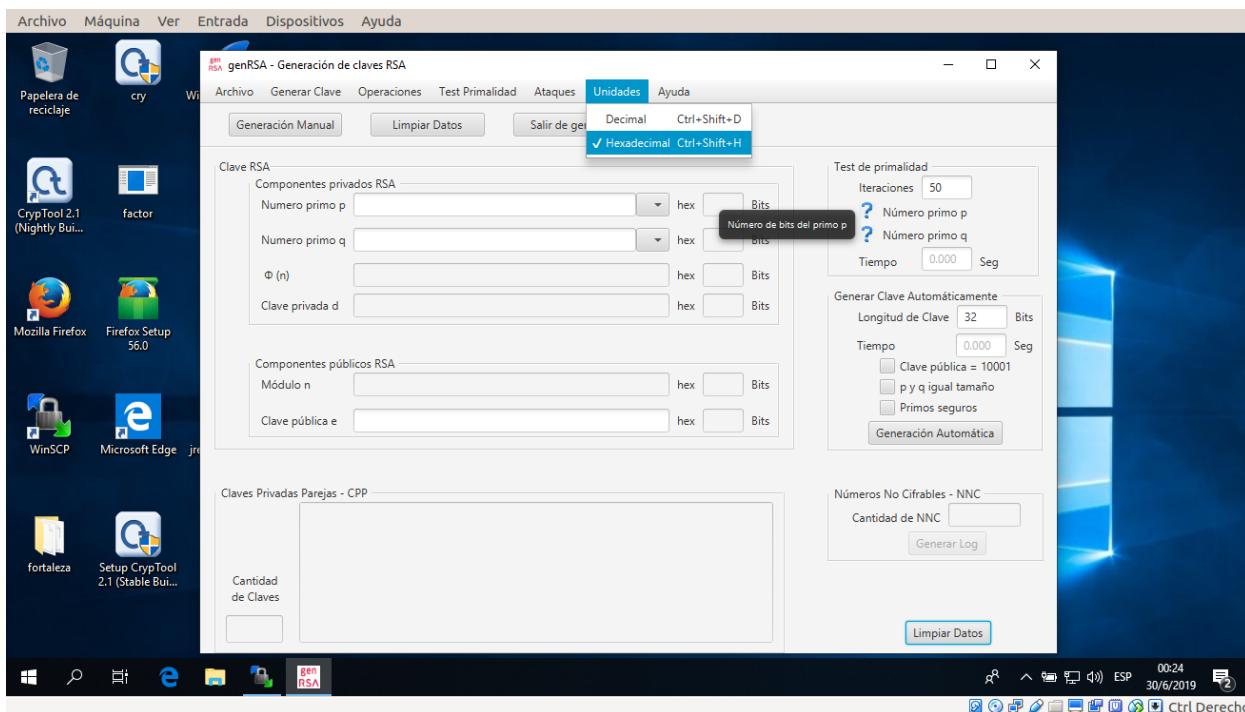


6. Saca conclusiones de lo observado.

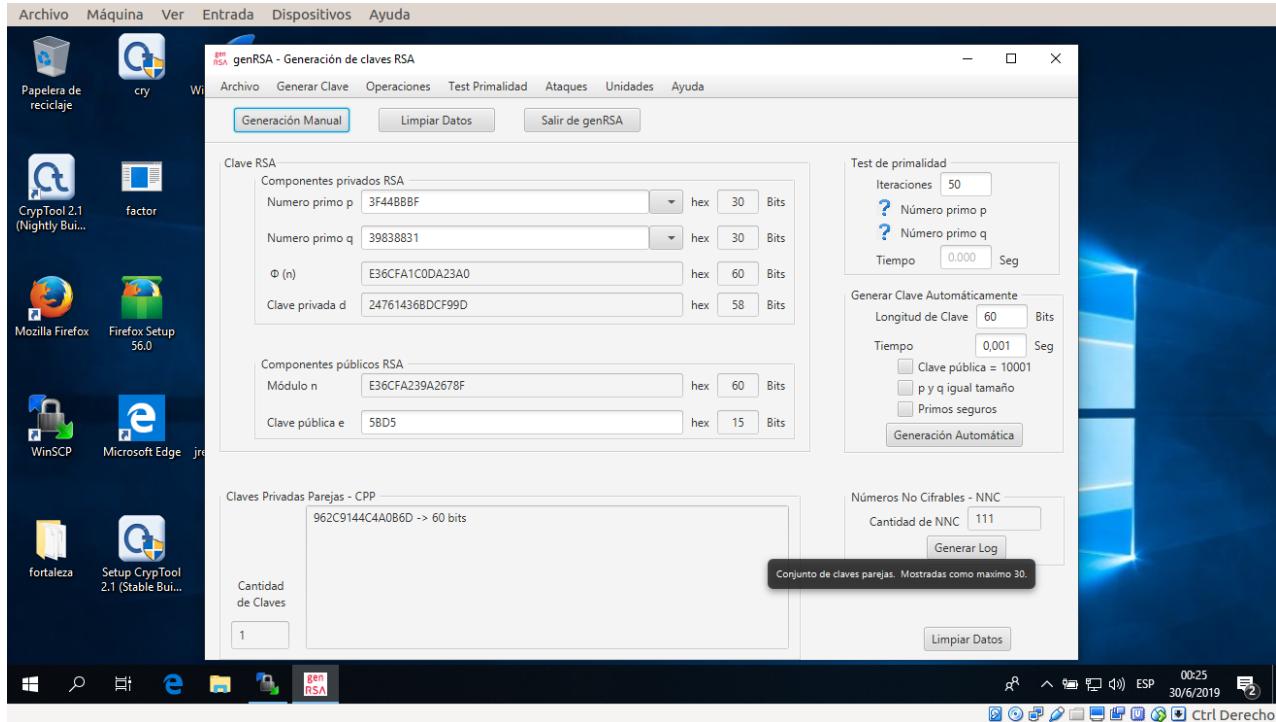
Como pudimos apreciar lo que realiza la opción p y q de igual tamaño es que ambos tenga la misma longitud de bits, ademas de que genera diferentes combinaciones de claves privadas parejas ademas que con esta opción activa solo varia de tamaño la clave privada d.

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 = 3F44BBBB.
5. q = 39838831.
6. e = 5BD5.
7. Desde la parte superior derecha de la aplicación, pulsa Generación Manual.
8. Saca conclusiones de lo observado.



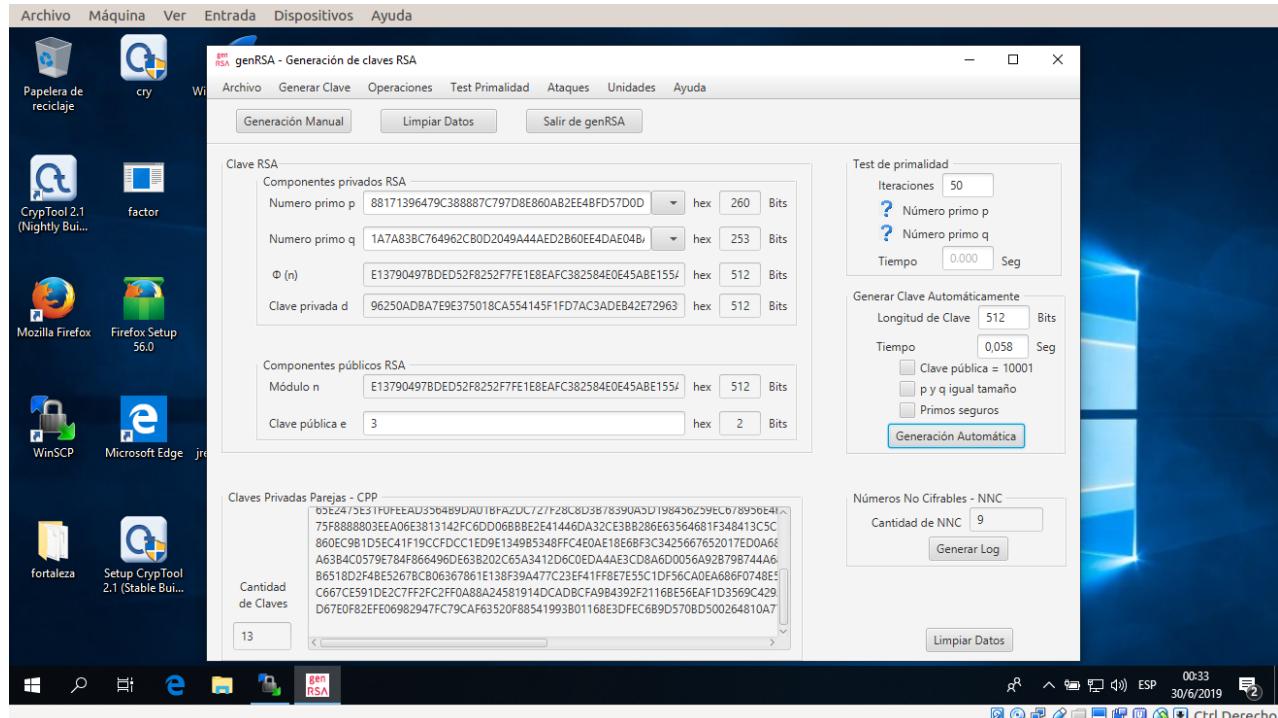
Conclusion:

Podemos apreciar que la mayoria de los valores introducidos son mayores en longitud comparado con pruebas anteriores ademas de que la clavee privada d es mayor en longitud que la clave publica e.

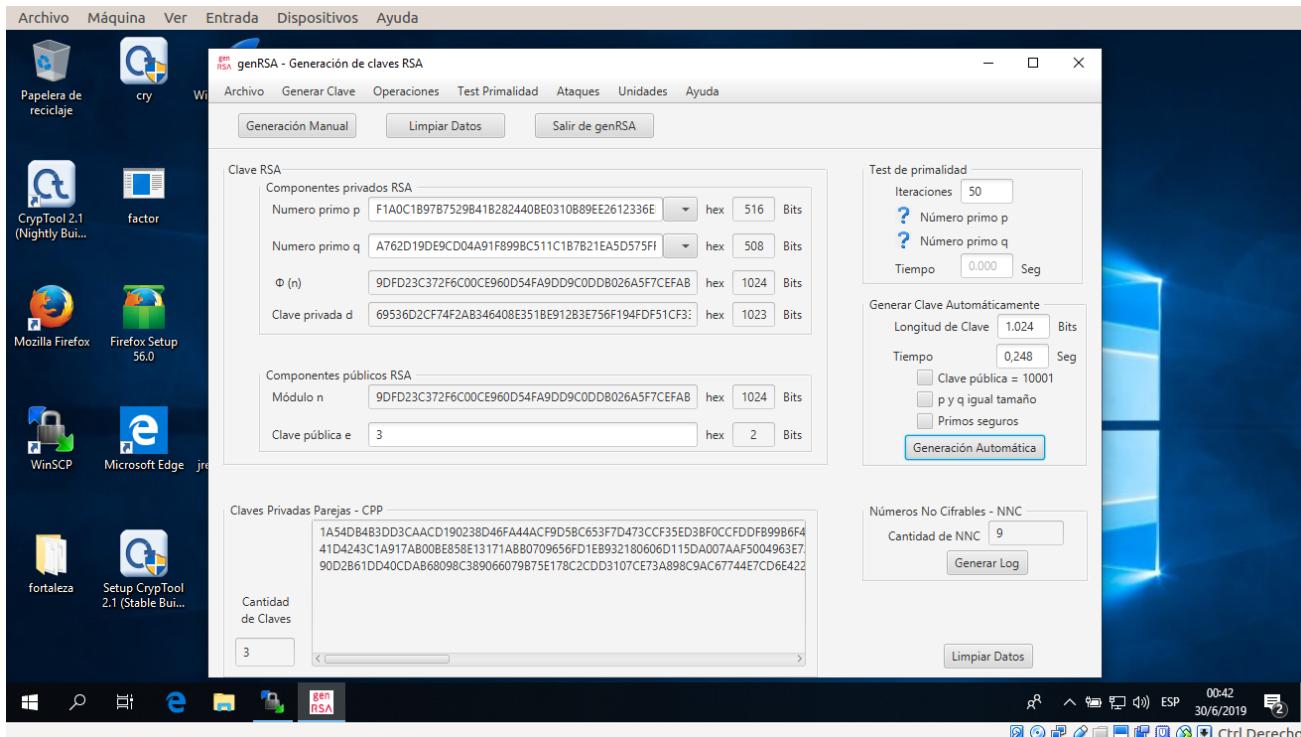
Paso 3:

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.

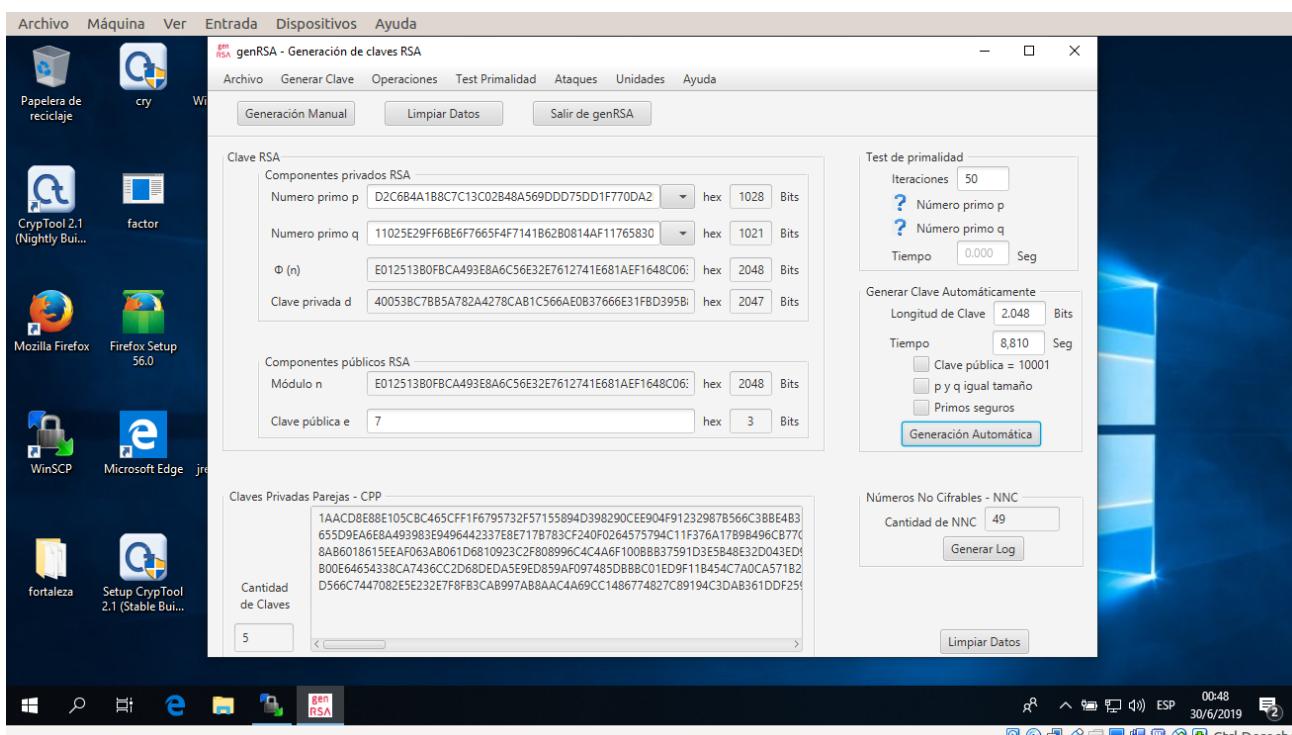
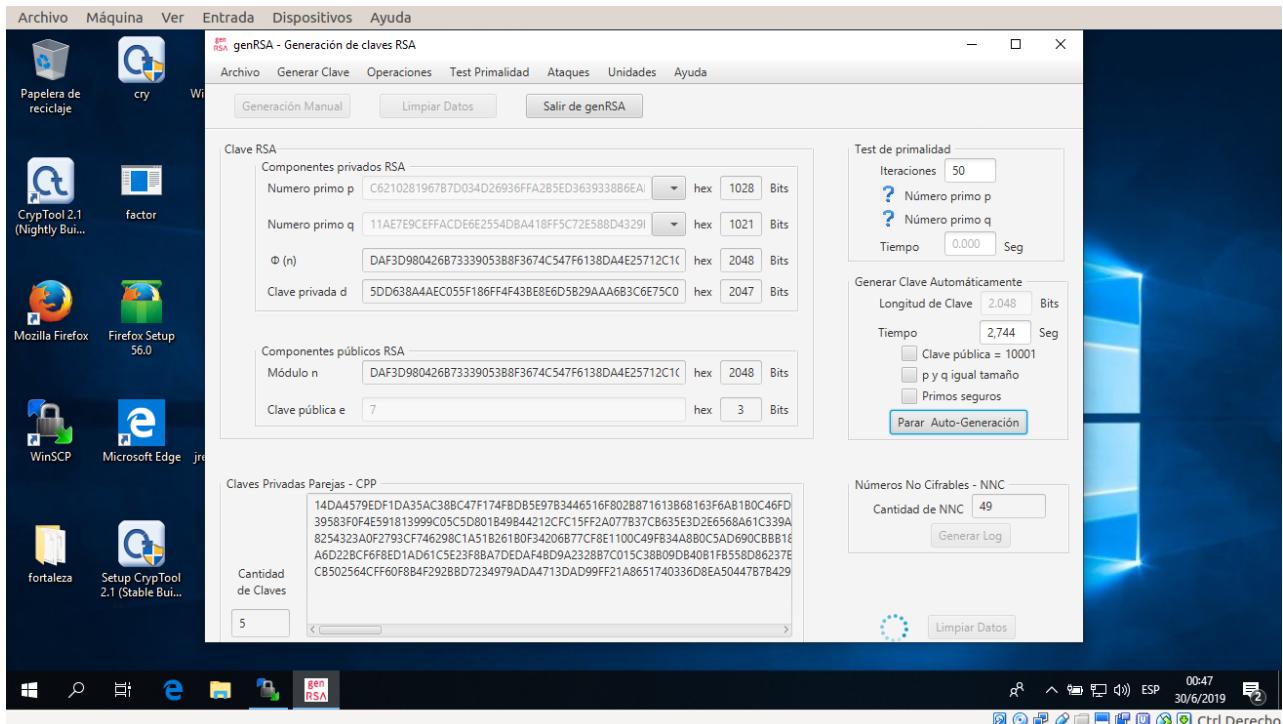
512



1024



2048



Conclusion:

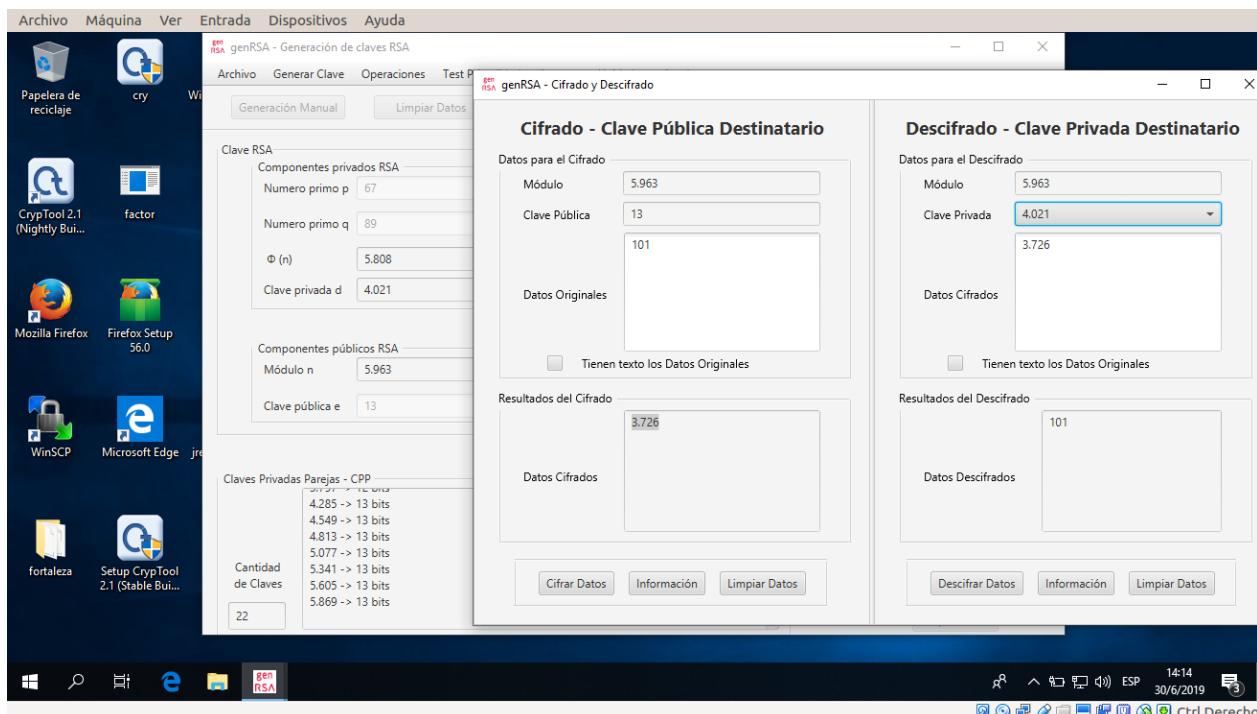
Para una longitud de clave tan larga se necesita datos de gran longitud tanto para p como para q ademas de que la clave publica ha sido apenas de 2 bits y 3 bits (longitud 2048) tambien podemos recalcar que la cantidad de numeros no cifrables con longitud de clave 512 y 1024 ha sido el minimo que estandariza

RSA y con longitud 2048 es de 49, mientras mas larga sea la clave mas tiempo se demora en calcular el resto de parametros como lo apreciado en la captura pasada.

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.

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



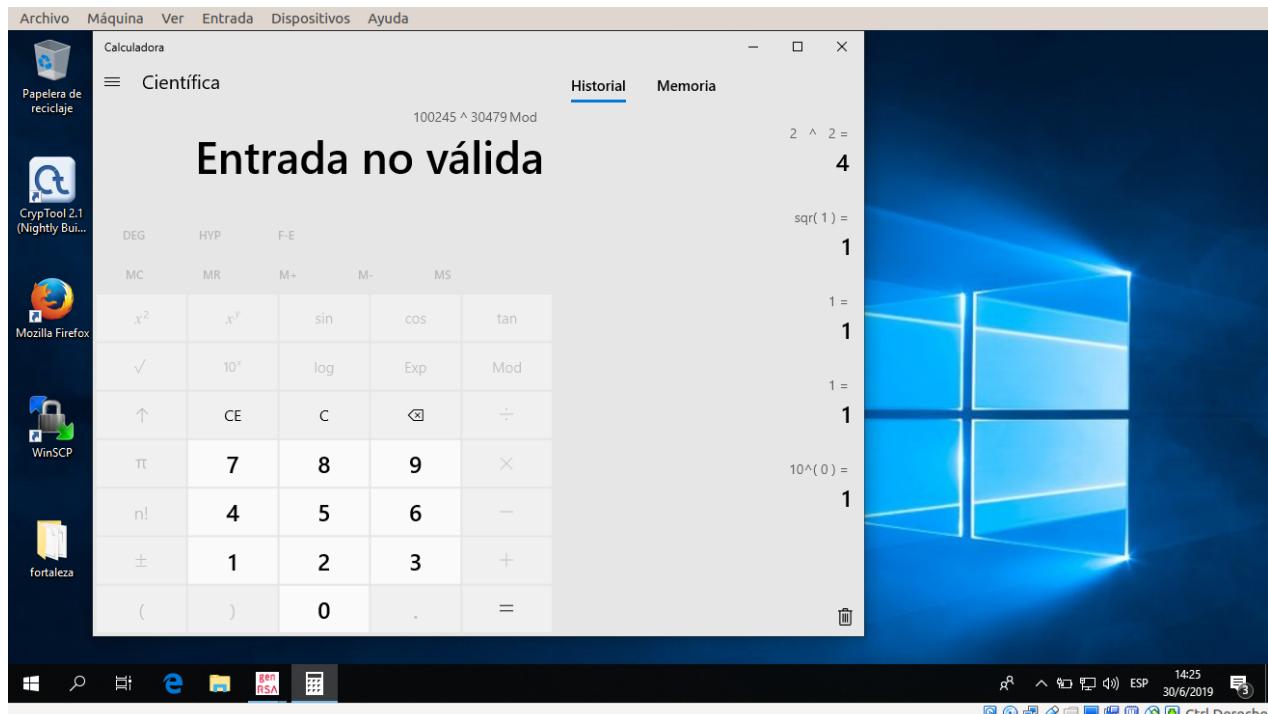
PrácticaRSA1.4.1

Intenta realizar la siguiente operación con la calculadora de Windows:

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

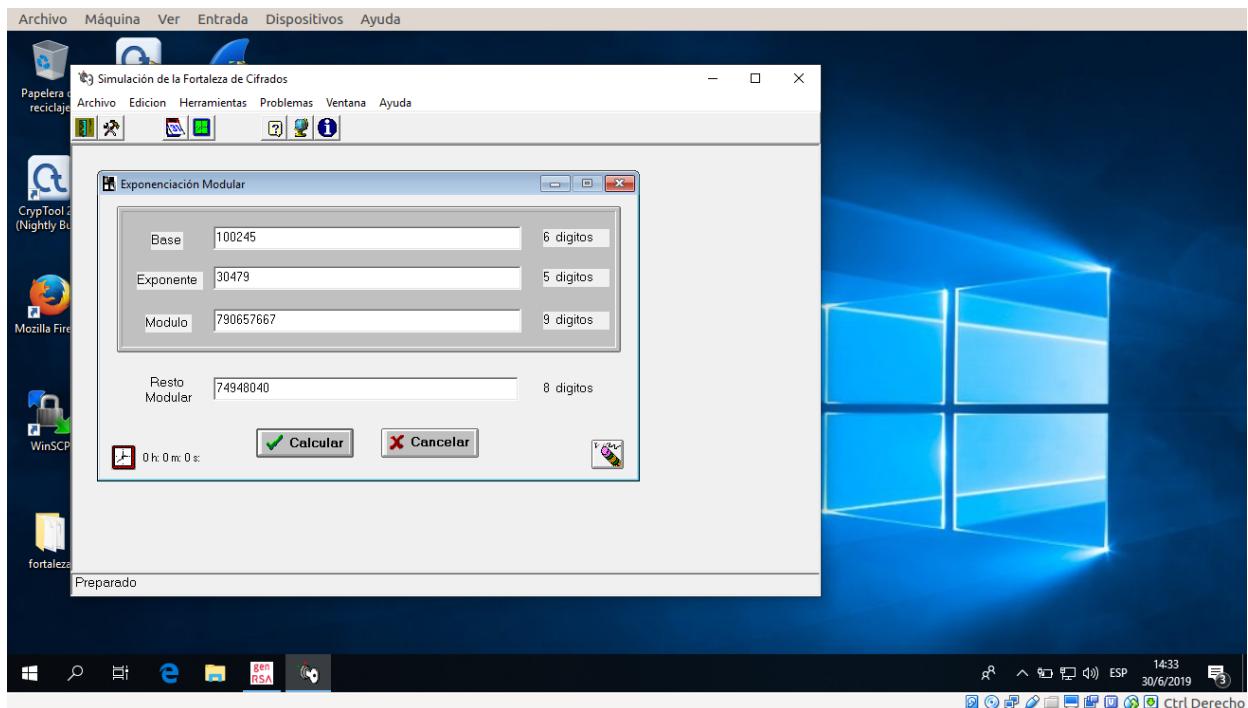
Los valores están indicados sin puntos para que puedas usar la opción de copiar y pegar.

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.

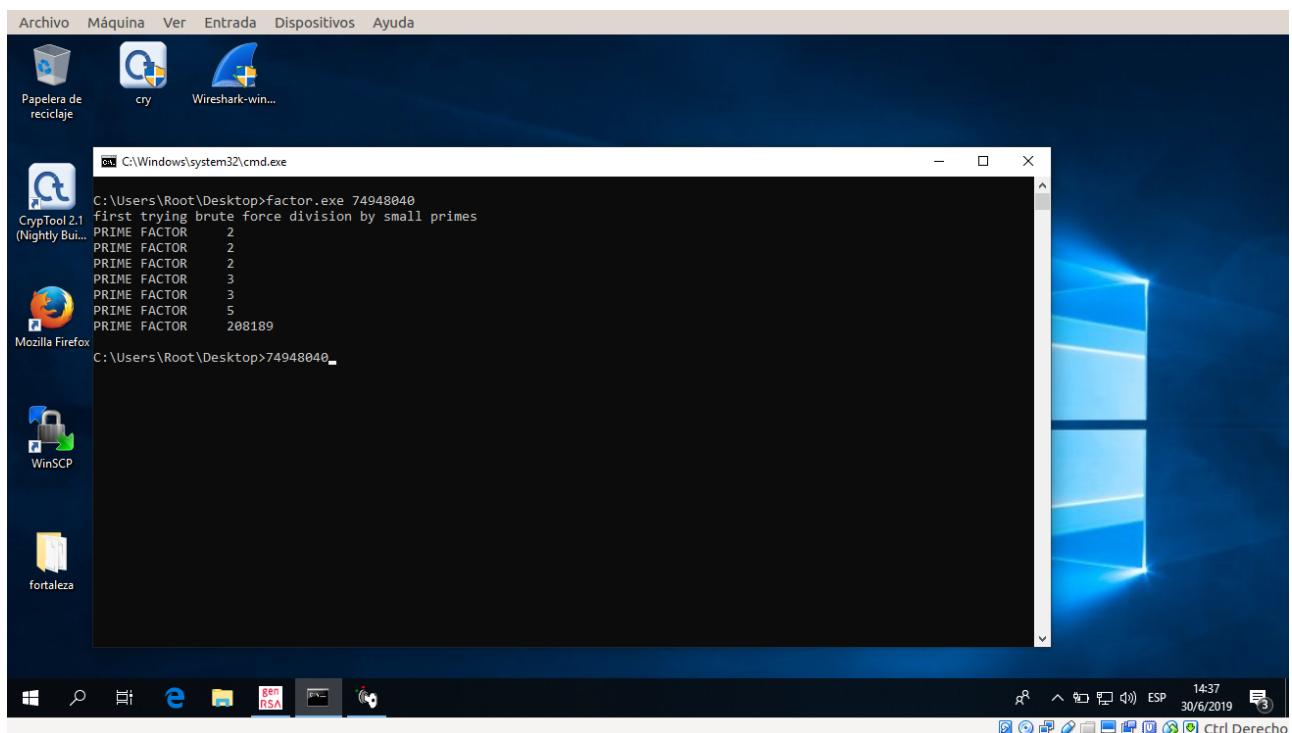


Operación Mod no válida en calculadora de Windows para números grandes

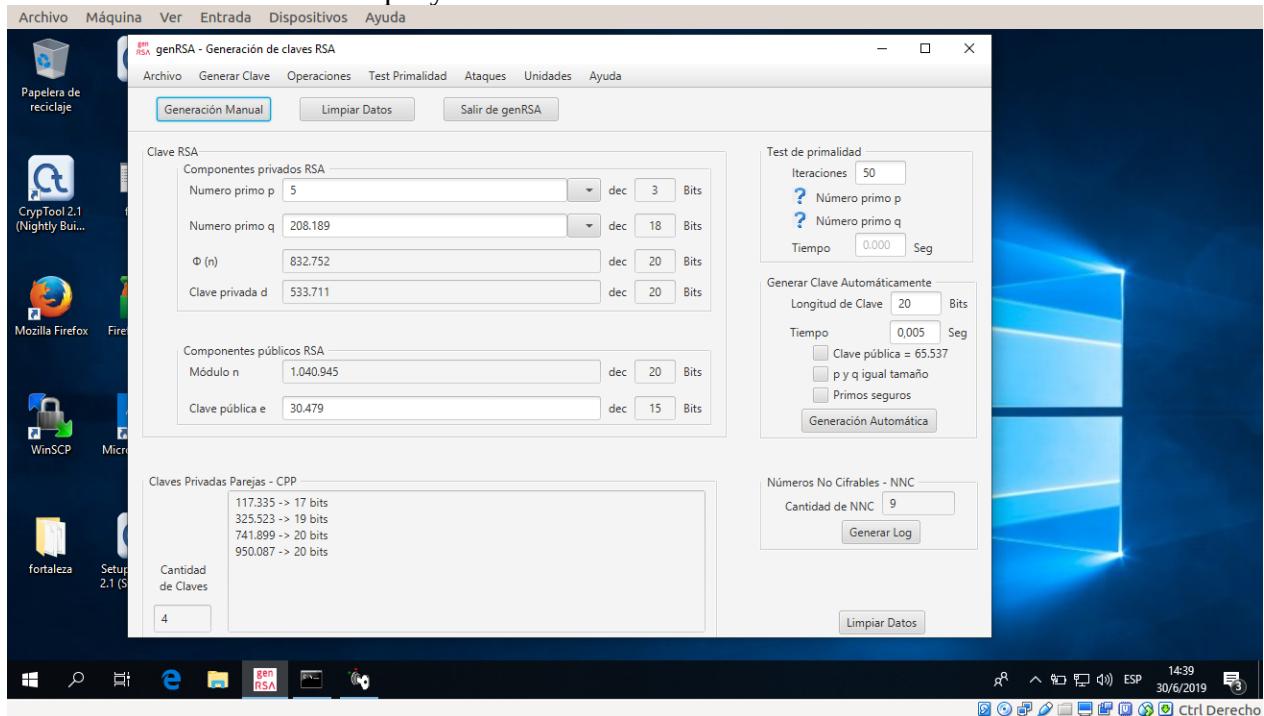
1. Comprueba que el resultado de la operación es 74.948.040.



2. ¿Cuáles serían los primos p y q de esta clave RSA?



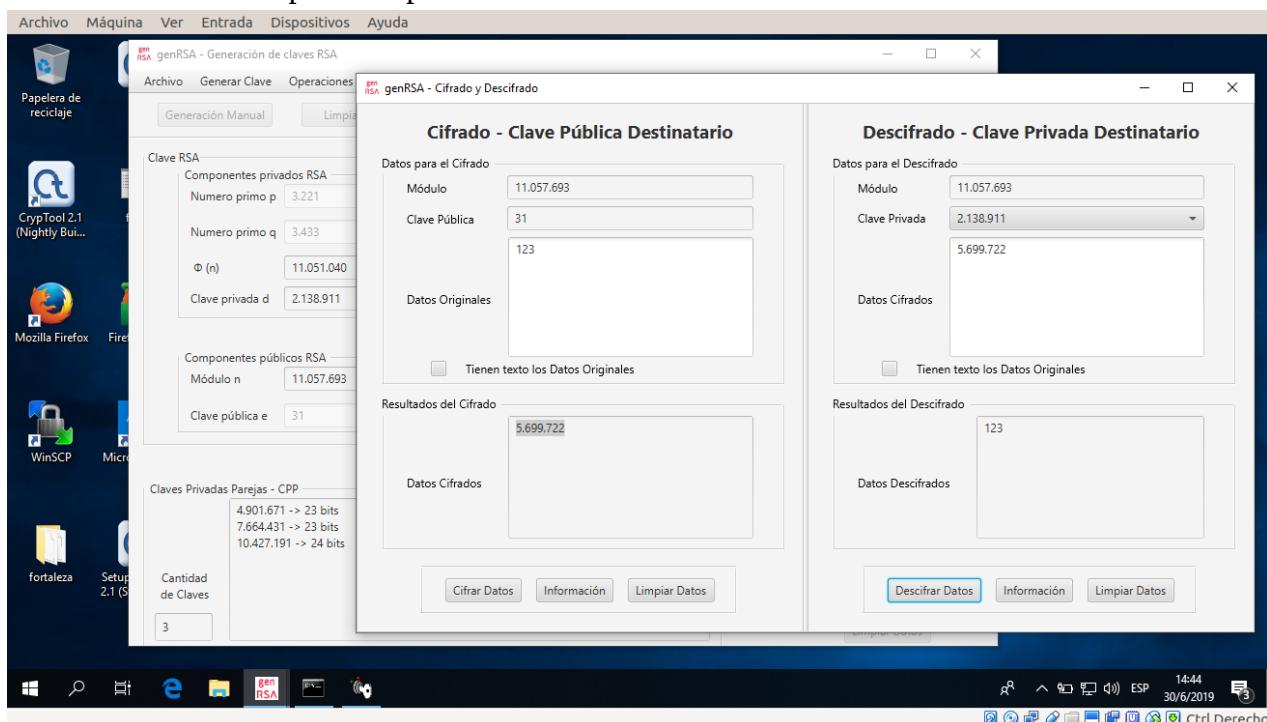
3. Si 30.479 es la clave pública e, ¿cuál es el valor de la clave privada d?
 Puedes usar el software que ya conoces.



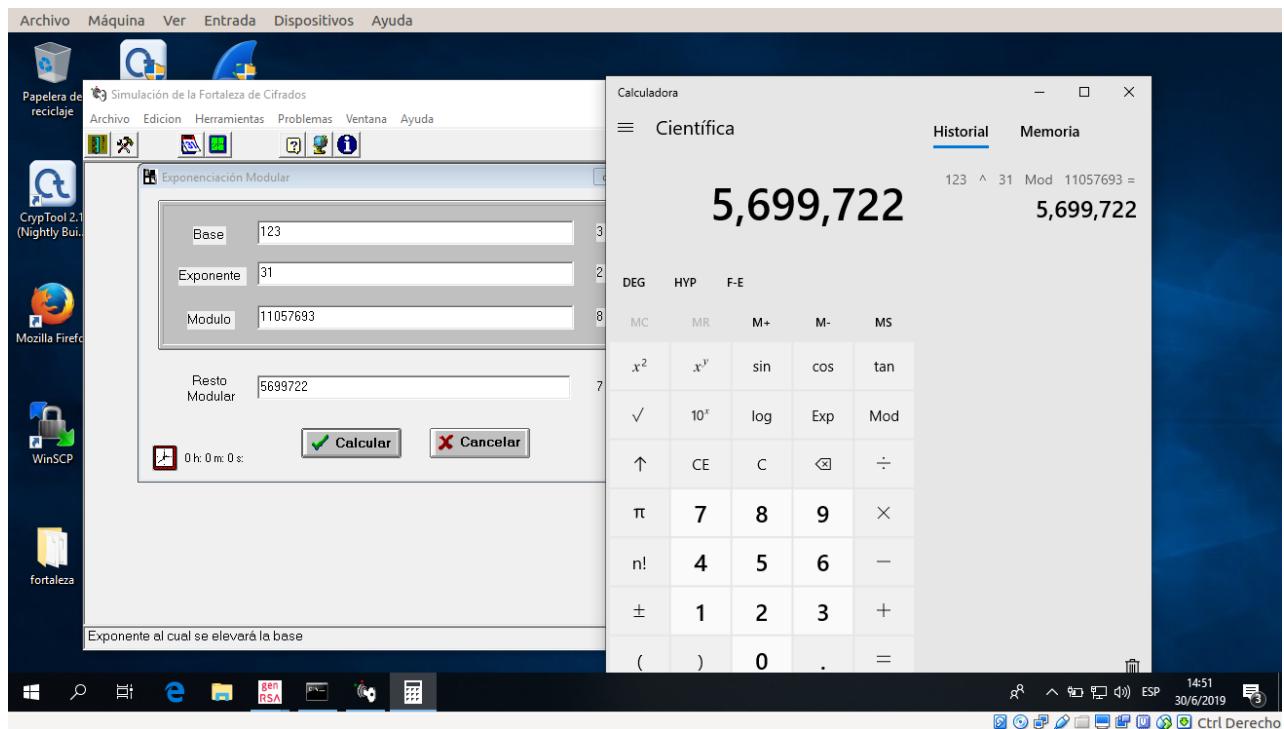
PrácticaRSA1.4.2

Usa el software genRSA para cifrar el siguiente mensaje.

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.



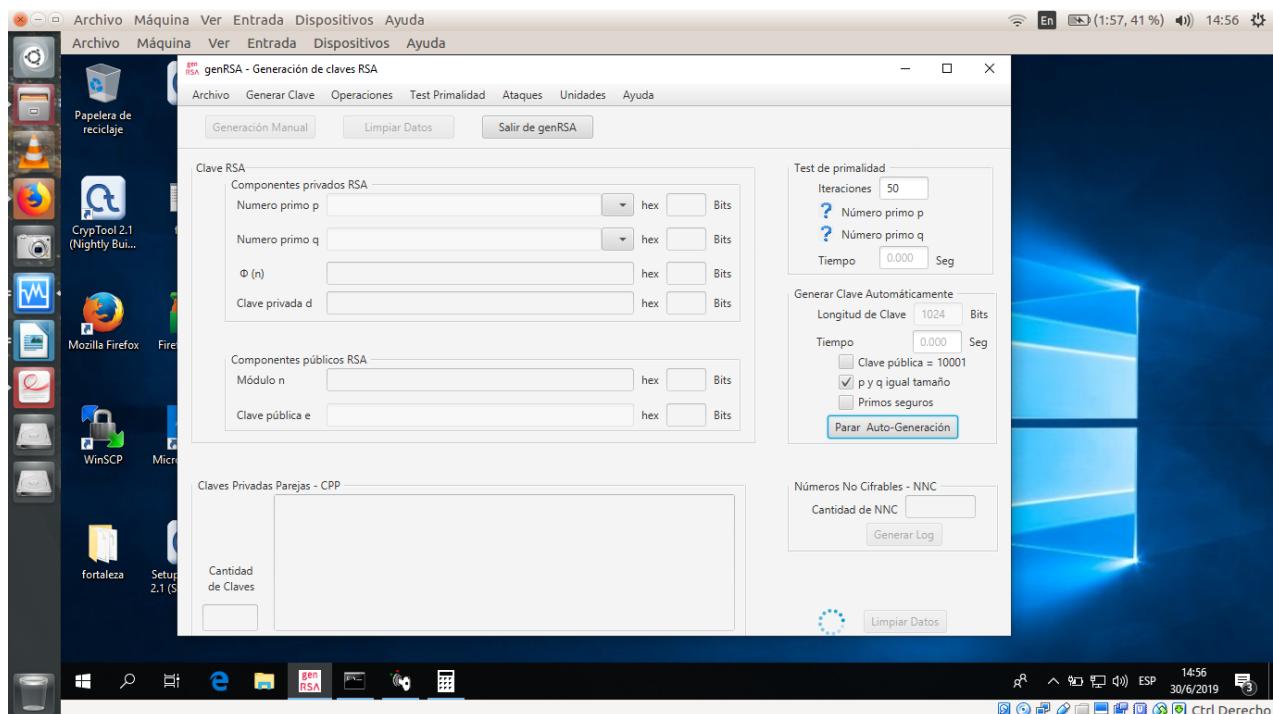
5. Comprueba este resultado con el software Fortaleza de Cifrados y con la calculadora de Windows.

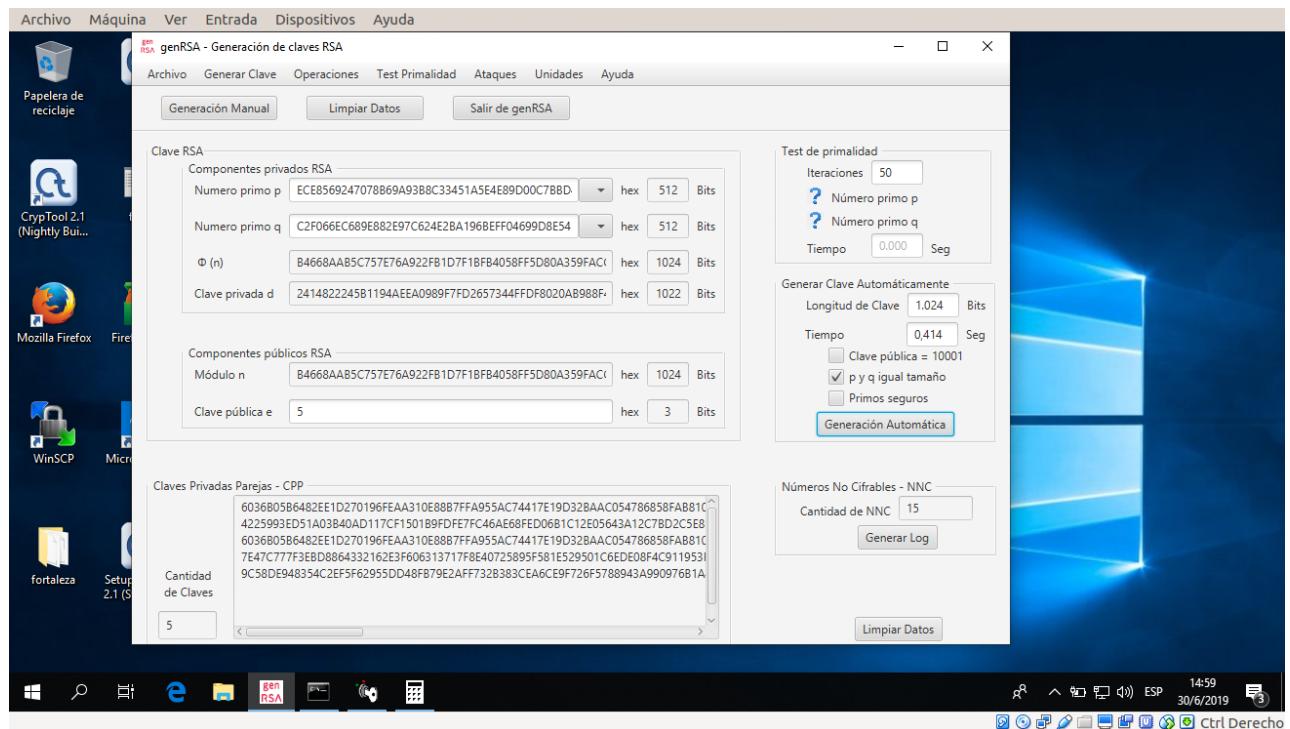


PrácticaRSA1.4.3

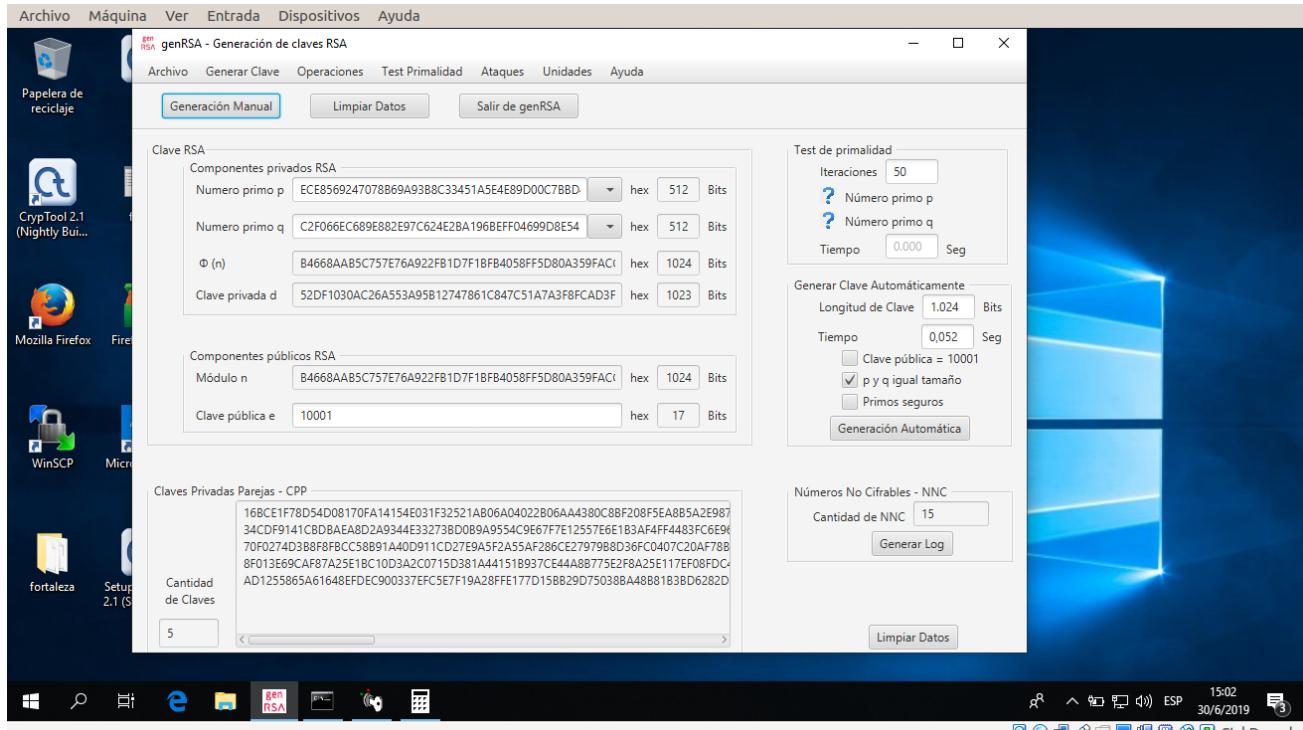
Usa el software genRSA y genera estas claves en hexadecimal.

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 ícono Generación Manual.



6. ¿Al cambiar la clave pública e, qué cosas cambian en la clave?

R: apesar de que el formato de clave ha sido cambiado su longitud de bits no varia, tambien pudimos observar que los bits a la izquierda fueron descartados de la clave ademas de que la clave privada ha aumentado 1 bit en su longitud.

7. ¿Qué tipo de clave "interesante" crees que has generado en esta sencilla práctica?

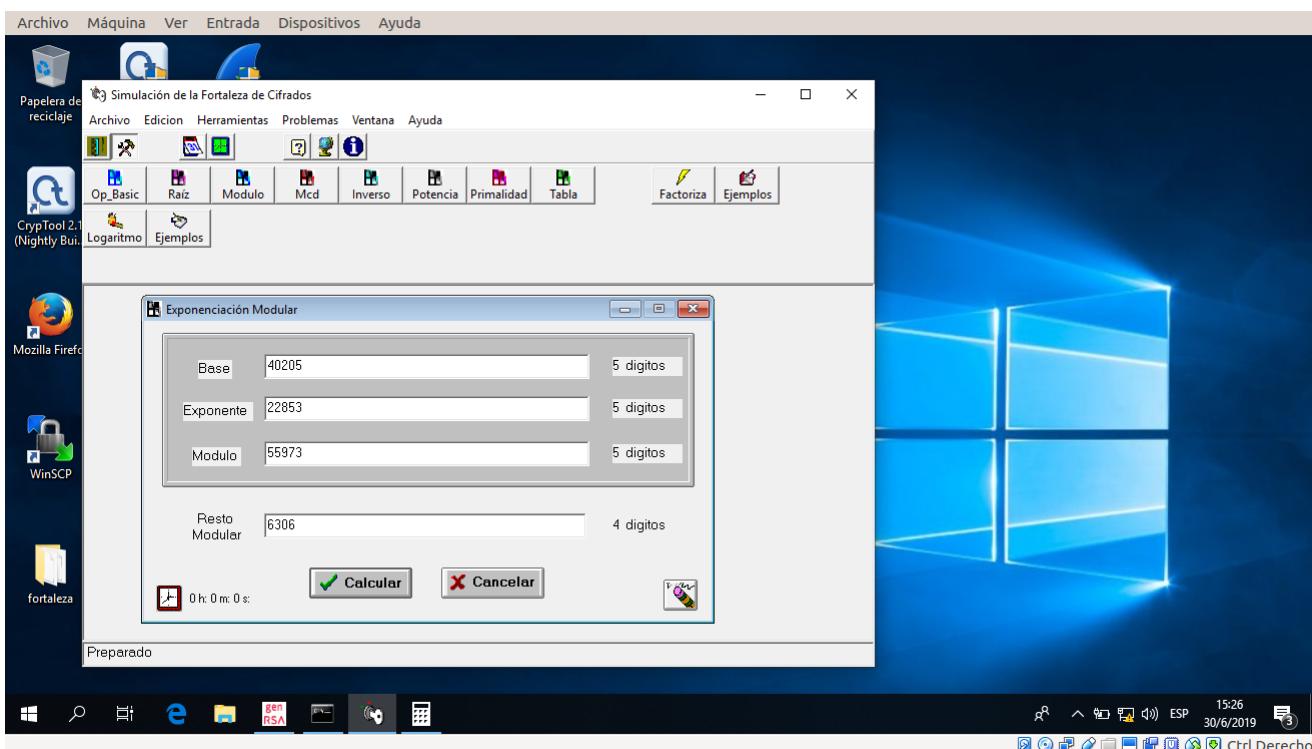
R: se ha generado una clave que elimina los bits innecesarios siendo estos bits a la izquierda.

PrácticaRSA1.5.1

Bernardo desea enviarle a Alicia firmado el valor 40.205. La clave pública de Bernardo es $^nB = 55.973$ y $^eB = 17$, y su clave privada $^dB = 22.853$.

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

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.

