CRYPT4YOU

DOCUMENTO ANEXO A LA LECCIÓN 2

DEL CURSO "EL ALGORITMO RSA"

EJERCICIOS Y PRÁCTICAS PROPUESTOS Y RESUELTOS

Autor: Dr. Jorge Ramió Aguirre
Fecha de publicación: 1 de abril de 2012
http://www.criptored.upm.es/crypt4you/temas/RSA/leccion2/leccion02.html

TABLA DE CONTENIDOS

LECCIÓN 2. VALORES DE DISEÑO DE LAS CLAVES

Apartado 2.1. Necesidad de un cuerpo de cifra mayor que 2.000 bits

ejercicioRSA2.1.1

- Accede a la página Web de un par de bancos de tu país y busca la banca online o que el enlace sea mediante SSL o TLS; es decir, que además de la indicación https en la url aparezca un candado amarillo en la parte superior de tu navegador si usas Internet Explorer, o bien un icono con el nombre del sitio Web al lado de la url que comienza por https si usas Mozilla Firefox.
- Repite el punto anterior para el navegador Chrome.
- Abre el certificado digital pinchando en ese candado amarillo en Internet Explorer o bien en el icono del banco al lado de la url en Mozilla Firefox.
- Observa en la pestaña Detalles que el sistema de cifra de clave pública que se usa es RSA y que el tamaño de la clave pública será muy probablemente de 2.048 bits.
- Desgraciadamente Firefox en sus versiones actuales ha quitado el famoso candado amarillo, tan característico de una conexión por plataforma segura cifrada mediante el protocolo SSL/TLS.

LECCIÓN 2. VALORES DE DISEÑO DE LAS CLAVES

Apartado 2.2. Relación tamaño clave pública versus clave privada

prácticaRSA2.2.1

- Con el software genRSA, genera manualmente las siguientes cuatro claves de 1.024 bits en hexadecimal.
  SW genRSA: http://www.criptored.upm.es/software/sw_m001d.htm
- Observa los valores que va tomando la clave privada d, en comparación con el tamaño del módulo n.
- IMPORTANTE: si haces doble clic con el ratón sobre los valores de p y q para copiarlos y pegarlos en genRSA, observa que el último carácter hexadecimal no lo incluye. Esto no ocurre en el archivo Word original, es un fallo de Adobe Acrobat al tratar cadenas largas. Para que genRSA no te muestre un mensaje de error, por favor incluye manualmente el carácter que falta en esos dos números.
  CLAVE 1: valores de p, q, e:
- CDB86A44510A34E8A49445E26D56F247401C2469F4F4FDF061E5BF2C68DEEAA934EDA504C0B15FFE9912B6CFE62F98BDA598A8EC37BEE3781FA883C107E72405
- C38FFB11305E29F674FB4CDA22238174E75B88961C2625034A7BC582EE766530794EB01A9B87670BC16906A3DDB0A5A965851CA29EAD6AA31A0158637F1E5A41
- 010001
  CLAVE 2: valores de p, q, e:
- FAAA690614E5710221029667BA1FC96B0E3D593871F5CF405D6717D1B774E0E9542D444BBC8AACD22E60EE06E48DB9ED9775332446B3E02D3408C60B3097D02D
- FED449D0F40D1E0866AEA099B4FC4D140025E743B678D5050FD4C758DA6199B87B7F7AA834FC4D8EA38A4FC38C70FAEBD97F2A82DF487FB8E38C027FDDF40D31
- 010001
  CLAVE 3: valores de p, q, e:
- C0DBECE07A7B7D194CD15541FF7383C0B113BEF88754F1C04FDCF71464AAA20AD2AA0308BB87E535FAC19B2D05FFFCF918A6AB3E90AA9CB495A5D3DAFB2670C3
- FB654BB843986C6E1B663E808A6986F29956B7B9708066696F9DFE0D7BCDB55696D8BEF9B3B7C052C857884D2499FB86039D4EAF604079330AE3E818FA6F7573
- 010001
  CLAVE 4: valores de p, q, e:
- F81AC7936444E1C2A2671B6AEC09F4DDD5BEC2E98D4A4A130F068E209B85E6DA6776521092CC0FDF591D68308D48CF82445B2CEAD0B47557ED667F1B3EDE159B
- D489EC4952C6EF58229FCBD3C3C57A9F18E1153E2634EA98C87AD0FCA415B7625D6783F30B801BCBE8F9BCFD4B1F94D7DB558C68FCB365408EF30677D78E16BB
- 010001

Apartado 2.3. Esquema de generación de claves con dos usuarios Alicia y Bernardo

ejercicioRSA2.3.1

Usando el algoritmo de exponenciación rápida resuelve las siguientes operaciones:

- $45^{17} \text{mod } 131$
- $25^{52} \text{ mod } 250$
- $100^{31} \text{ mod } 121$

En los casos es suficiente el uso de la calculadora de Windows para cada una de las operaciones.

prácticaRSA2.3.1

Con el software Fortaleza de Cifrados realiza los siguientes cálculos, usando la opción copiar y pegar, y observa el tiempo que tarda en entregar la respuesta. La operación a realizar es A^B mod C que verás en las herramientas como icono "Potencia".

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

Elige como módulo un número aleatorio cualquiera y el máximo de dígitos que acepta el programa, es decir 300.

Caso 1: Base de 50 dígitos y exponentes de 25 dígitos, 50 dígitos, 100 dígitos y 150 dígitos.

Caso 2: Base de 100 dígitos y exponentes de 25 dígitos, 50 dígitos, 100 dígitos y 150 dígitos.

Caso 3: Exponente de 50 dígitos y base de 25 dígitos, 50 dígitos, 100 dígitos y 150 dígitos.

Caso 4: Exponente de 100 dígitos y base de 25 dígitos, 50 dígitos, 100 dígitos y 150 dígitos.

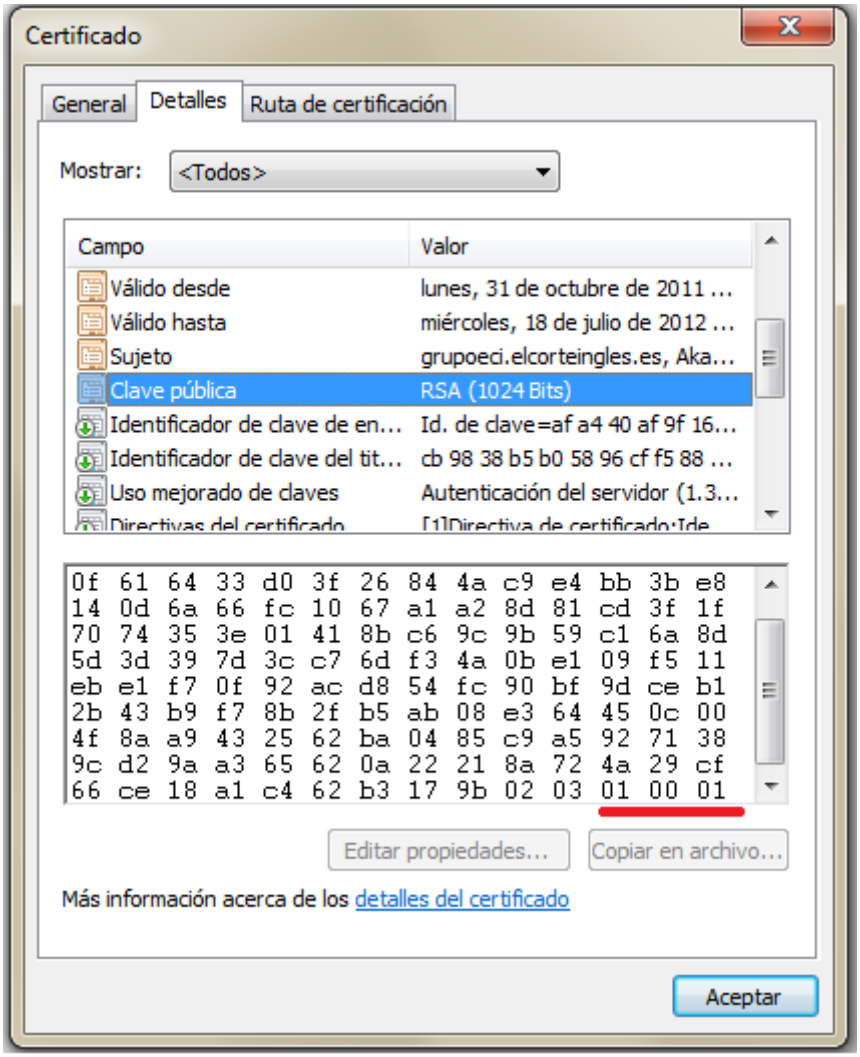
Caso 5: Base: 65378767658876582908768576298762092138; Exponente: 65537.

Saca conclusiones de los tiempos de cálculo encontrados en los Casos 1 al 4.

prácticaRSA2.3.2

Con Internet Explorer se pide abrir el certificado digital X.509 que aparece al forzar pagar con tarjeta una compra en la página Web de estos Almacenes: http://www.elcorteingles.es
Pon artículos en el carrito de compra y luego indica Tramitar Pedido para entrar en una conexión segura.

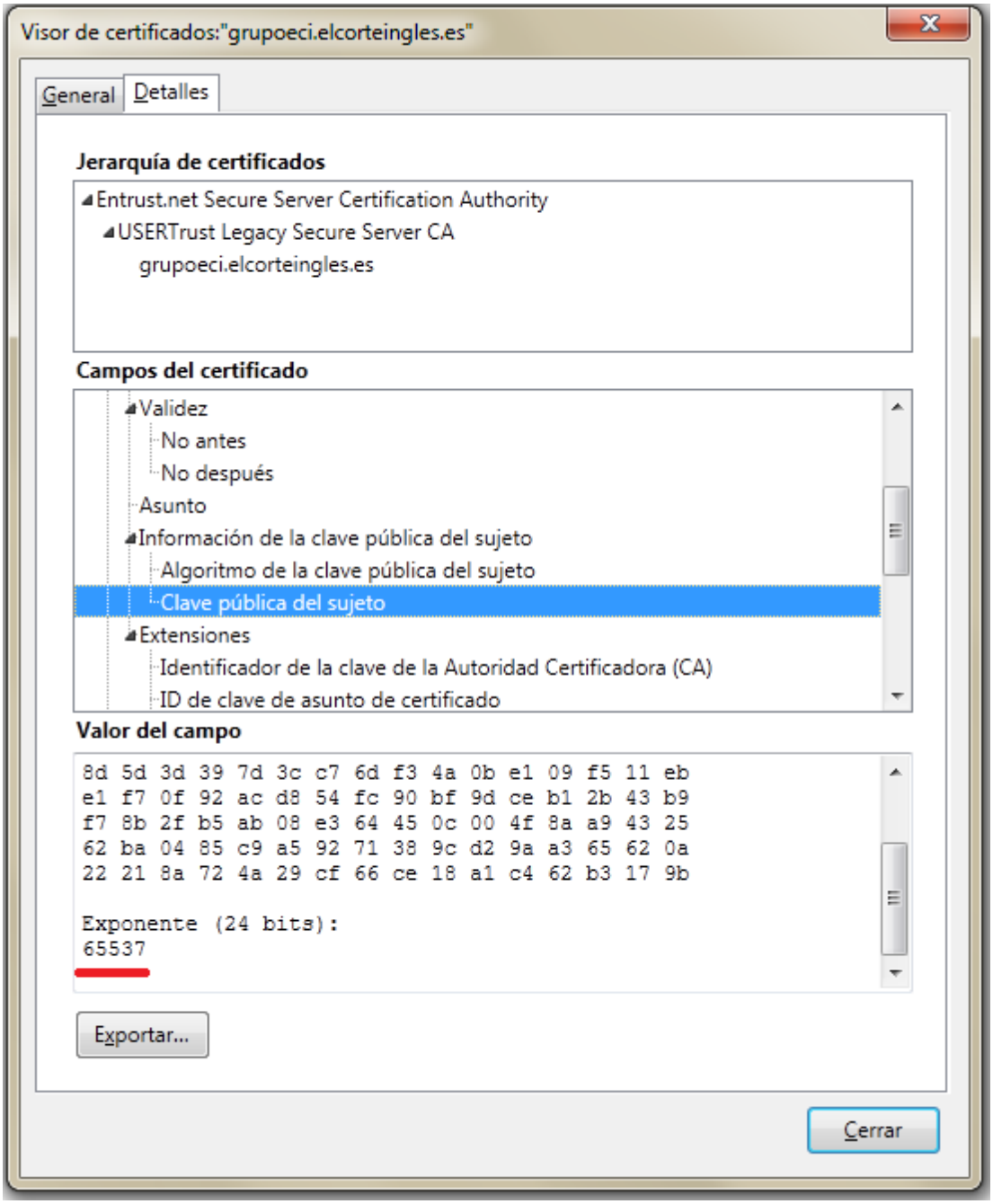
- Comprobar que la clave pública e es F_4 y ver en qué formato la entrega cada navegador. Mostrar el valor de la clave pública.



Clave pública e en formato hexadecimal de 24 bits en Internet Explorer: fecha de acceso 30/12/2011. La palabra 0203 es un código que indica que a continuación viene el valor e. No forma parte del valor de n que, en este caso, termina con 179b.

Usando ahora Firefox como navegador, abre el certificado digital X.509 que aparece al repetir el ejercicio a en la página Web de estos Almacenes: http://www.elcorteingles.es
Pon artículos en el carrito de compra y luego indica Tramitar Pedido para entrar en una conexión segura.

- Comprobar que la clave pública e es F_4 y ver en qué formato la entrega cada navegador. Mostrar el valor de la clave pública.



Clave pública e en formato decimal que muestra Mozilla Firefox: fecha de acceso 30/12/2011.

Apartado 2.4. ¿Qué pasaría su usamos cualquier valor válido de e?

prácticaRSA2.4.1

Con el software genRSA genera las siguientes claves, en la que se elige un valor de e aleatorio muy alto, cercano al módulo n pero válido.

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

Valores de p, q, e:

- EE0F219CCB4BCDB17AB66B7D692F6E72D25CEE16B293FE06C3FB3A3BABEE9FCF
- CBE21DB30DD956EDF1BD43A0AB58530FBF35B34465B614BA7761AE5A8E7B8637
- 1B15C0A95169D14B68CD96E03C138EC4C9EF3F5E78ACE81FA01D34A801C9AA212DE4 5049B5DDE65DEECEC263C94804976ECE8A0BB120902CFB02CFE6512313A3

- F33AE998463DC0AE6EC378E8DD5E2B86207C5D89873B8522CB7FCA6AF4410A85
- FAD3BDAC07EE025BC0AF3B802642724CB40717BD7C96F4C6BE0164AAB959C12D
- EE50B5E32EAD50A0E90250845FC7D96C9E7E20AA09330E7A16A874477EACFE468887 F82BB097BB6C79C1237321DE8F7559F7A148CAE20E9B2295127ABD9A1E61

¿Qué ha pasado con la clave privada d?

Genera de forma automática una clave de 1.204 bits.

Copia el valor de la clave privada d al portapapeles, pégala en la ventana de la clave pública e y genera esa clave ahora manualmente.

Repite los dos pasos anteriores para una clave de 2.048 bits.

¿Serían débiles estas claves?

prácticaRSA2.4.2

Con genRSA genera estas tres claves de 24 bits en que e es $\phi(n)/k + 1$ con k = 2, 3, 4, ... y es una clave válida: mcd [e, $\phi(n)$] = 1.

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

Observa lo que sucede con el número de mensajes no cifrables y saca conclusiones de lo observado.

- Clave 1 usando k = 2: p = 3049; q = 3491; e = 5318761.
- Clave 2 usando k = 4: p = 3049; q = 3491; e = 2659381.
- Clave 3 usando k = 6: p = 3049; q = 3491; e = 1772921.
- Clave 4 usando k = 8: p = 3049; q = 3491; e = 1329691.

Las clave generadas con un valor de e válido que cumple además con la relación $e = \phi(n)/k + 1$, donde k = 2, 3, 4, ... tienen el comportamiento que acabas de comprobar.

Por tanto, es necesario que la clave pública esté de alguna manera controlada y por ello se establece el valor estándar el número 4 de Fermat para todo el mundo.

Ese número es muchísimo más pequeño que $\phi(n)$ y, por tanto, ese posible valor k es inmenso y en ese rango ya no se observa este fenómeno.

Apartado 2.5. Aspectos a tener en cuenta en la elección de los primos p y q

ejercicioRSA2.5.1

Con el software Fortaleza de Cifrados multiplica por sí mismo este número de 116 dígitos (384 bits) que corresponde el valor del primo p del último desafío RSA 768 resuelto en el año 2009.

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

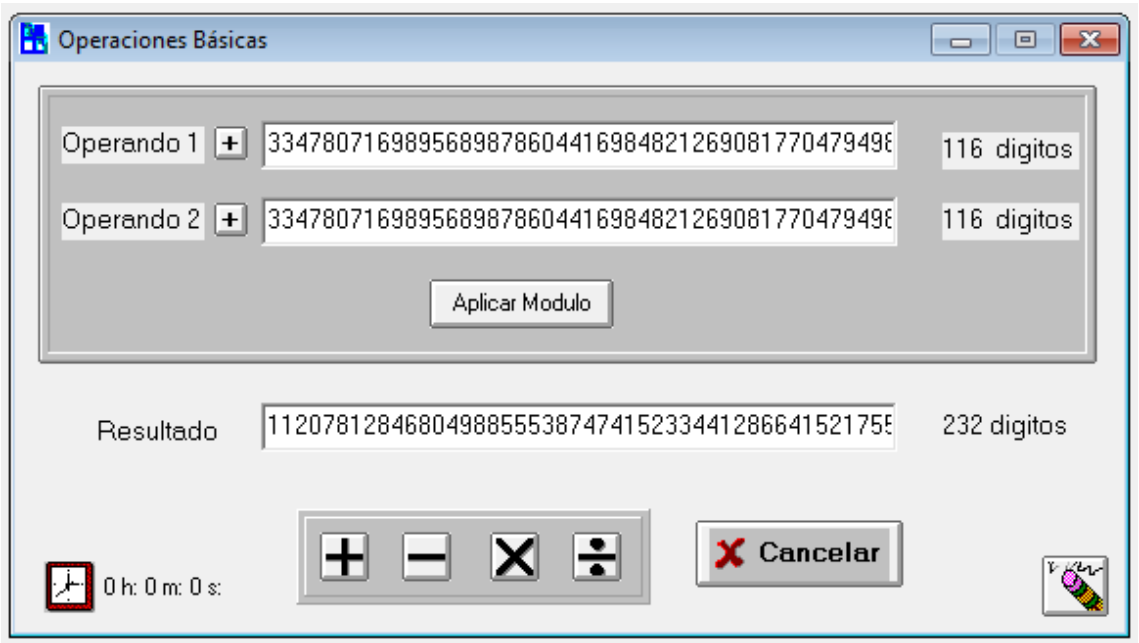
334780716989568987860441698482126908177047949837137685689124313889828837938780022876147116525317430877378144679994 89

Observa el producto resultante de 232 dígitos (768 bits).

Hecho esto, con esta calculadora encuentra la raíz cuadrada de ese número de 768 bits.

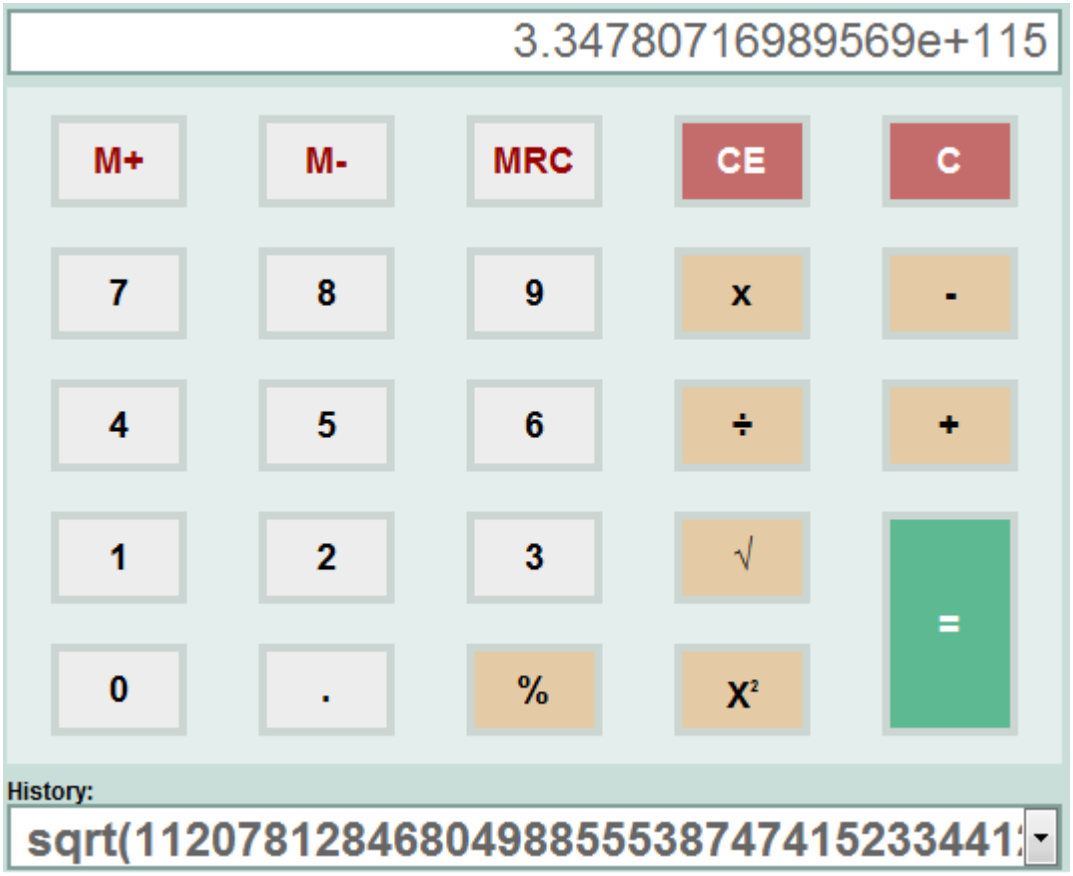
Web: http://calculator.pro/Scientific_calculator_online.html

Si multiplicamos ese número primo por sí mismo, obtenemos el siguiente resultado:



Multiplicación de dos números primos iguales de 384 bits y su producto de 768 bits

Si ahora usamos la calculadora científica online para encontrar la raíz cuadrada de ese número, obtenemos precisamente el valor del primo p como se observa.



Cálculo online de la raíz cuadrada de un número de 768 bits resultado de elevar al cuadrado un número primo de 384 bits, con un tiempo de ejecución inmediato.

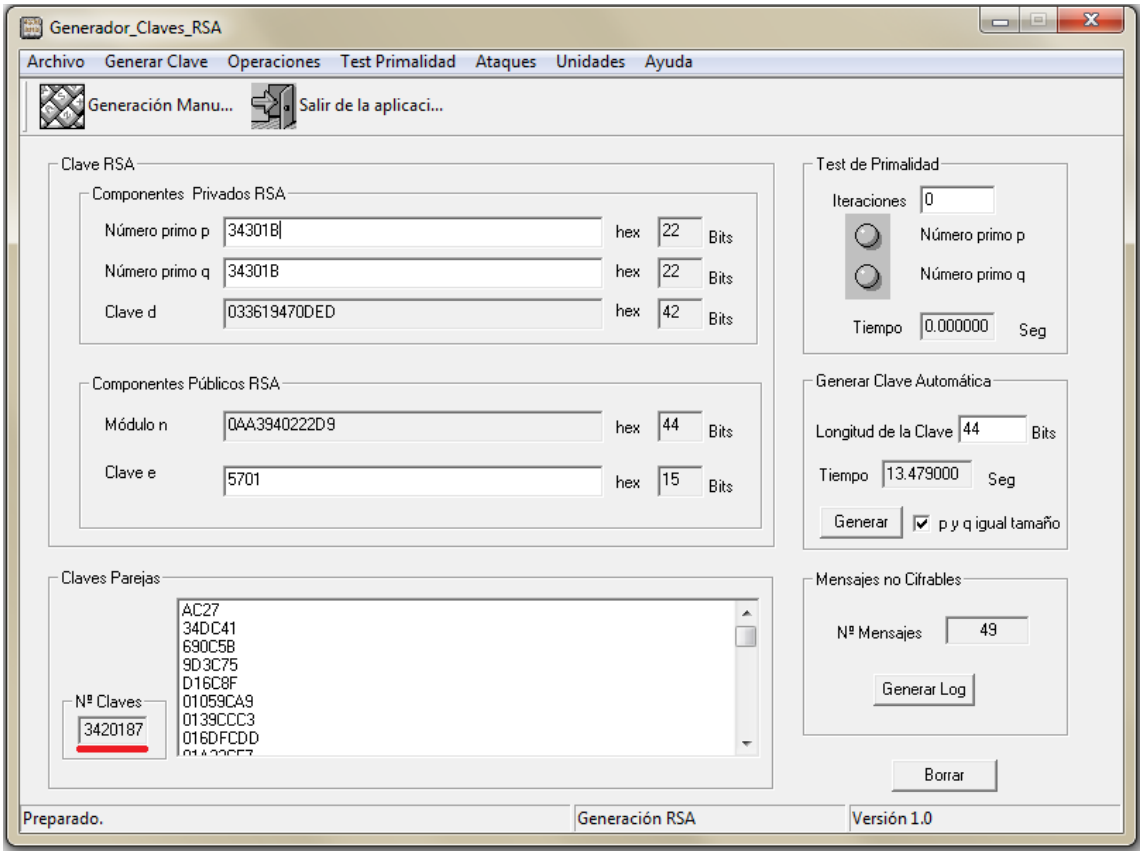
prácticaRSA2.5.1

Con el software genRSA y genera manualmente estas tres claves y observa qué sucede con las claves privadas parejas que indica el programa.

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

- Clave decimal de 14 bits: p = 101; q = 101; e = 37.
- Clave decimal de 30 bits: p = 24989; q = 24989; e = 31.
- Clave hexadecimal de 44 bits: p = 34301B; q = 34301B; e = 5701.

Nota: En este último caso, el programa tardará varios minutos en entregar la respuesta, indicando además durante su ejecución que la aplicación "No responde". No hagas caso de ello; es debido a que existirán 3.420.187 (valor decimal de 34301B) claves privadas parejas y debe escribir todos esos valores en la ventana correspondiente, como se muestra en las siguientes figuras.



Clave hexadecimal de 44 bits con valores de p y q iguales

prácticaRSA2.5.2

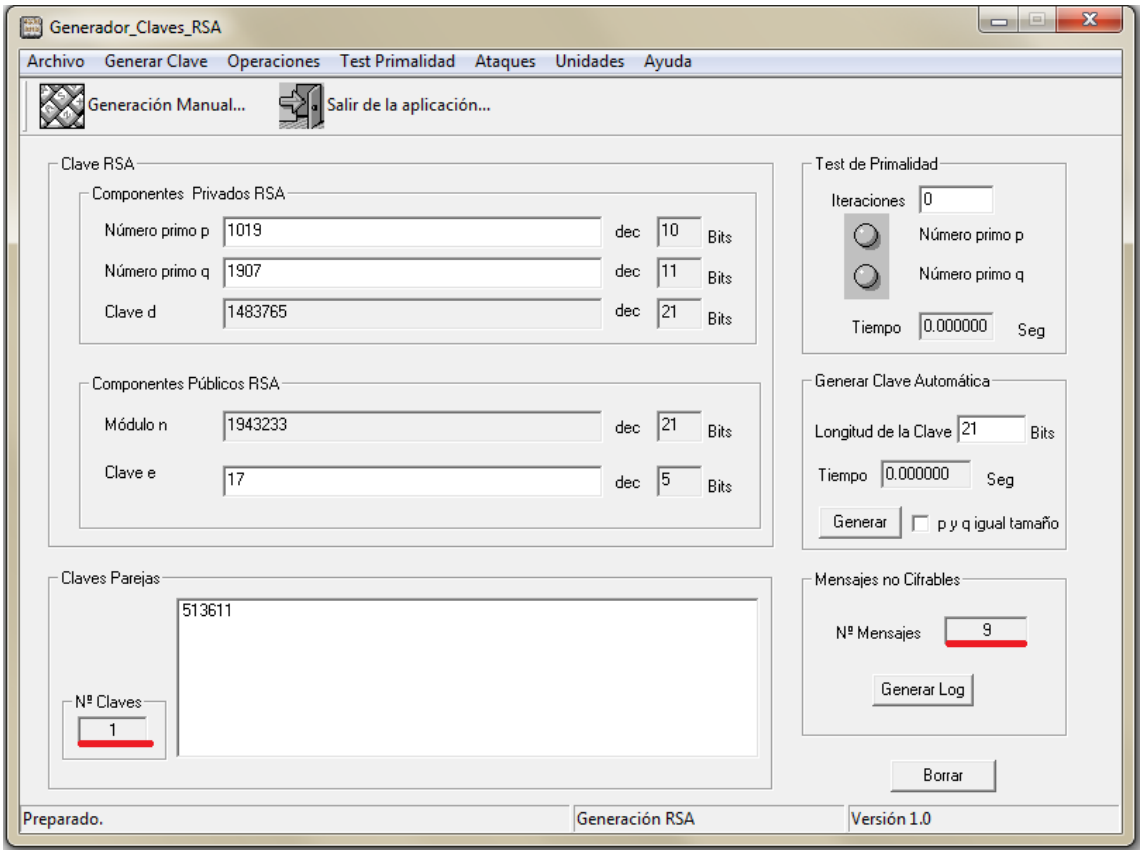
Con genRSA genera manualmente estas tres claves con primos seguros y observa qué sucede con el valor de las claves privadas parejas y los mensajes no cifrables.

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

No te preocupes por querer entender ahora qué son las privadas parejas y los mensajes no cifrables, esto se estudiará en las lecciones 5 y 6.

- p = 23; q = 83; e = 31.
- p = 1019; q = 1907; e = 17.
- p = 13043; q = 14159; e = 131.

¿Por qué son primos seguros 23, 83, 1.019, 1.907, 13.043 y 14.159?



Clave óptima generada con primos seguros

prácticaRSA2.5.3

Repite con genRSA la práctica anterior usando ahora estos primos fuertes y comprueba que no se obtienen claves RSA óptimas.

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

- p = 29; q = 71; e = 13.
- p = 137; q = 223; e = 29.
- p = 331; q = 499; e = 37.

¿Por qué son primos fuertes 29, 71, 137, 223, 331 y 499?