CRYPT4YOU

DOCUMENTO ANEXO A LA LECCIÓN 4

DEL CURSO "EL ALGORITMO RSA"

EJERCICIOS Y PRÁCTICAS PROPUESTOS Y RESUELTOS

Autor: Dr. Jorge Ramió Aguirre
Fecha de publicación: 4 de mayo de 2012
http://www.criptored.upm.es/crypt4you/temas/RSA/leccion4/leccion04.html

TABLA DE CONTENIDOS

LECCIÓN 4. CLAVES PRIVADAS Y PÚBLICAS PAREJAS

Apartado 4.1. ¿Qué son las claves privadas parejas?

prácticaRSA4.1.1

Con el software genRSA, genera las siguientes claves y observa las claves privadas parejas que se indican en la zona inferior izquierda de la aplicación.
Números sin puntos para que puedas usar la opción de copia y pegar.
SW genRSA: http://www.criptored.upm.es/software/sw_m001d.htm

Claves en decimal:
Clave 1: p = 37, q = 41, e = 13.
Clave 2: p = 191, q = 223, e = 17.
Clave 3: p = 51169, q = 59009, e = 4063.

Claves en hexadecimal:
Clave 1:
p = F624F34384DE6A2741B6FD66E3F320B1
q = DCC48F2C0A4157554B8B9681475347F3
e = 32B7
Clave 2:
p = 038F1911BB3BB11B6CF74C1F22D5FA7F036CC5AD0ED4379AB8B81D72D7AD11
q = 2F82644AE5E0794298318465A5ECF379862DC09EB02B99DED06A3F0554322CB32D51
e = 38DD
Clave 3:
p =
E2288002909A8DEFC63738AD930088F5552CEF3E3983233EAE0829AD1ADAB24CCB5CAB2630
94101549D101895C911785EAA1F8EAE18629F8131C2412E77DAC65
q =
CD33DAE6EAD1F5EE0338EBC97EE0E64503A5DBD25312C0E420DFF99922B8139C6741B449EB
56D212689724216F24D63EB8A581F4B78E5AEF6FA1AAA98BB47ED9
e = 010001

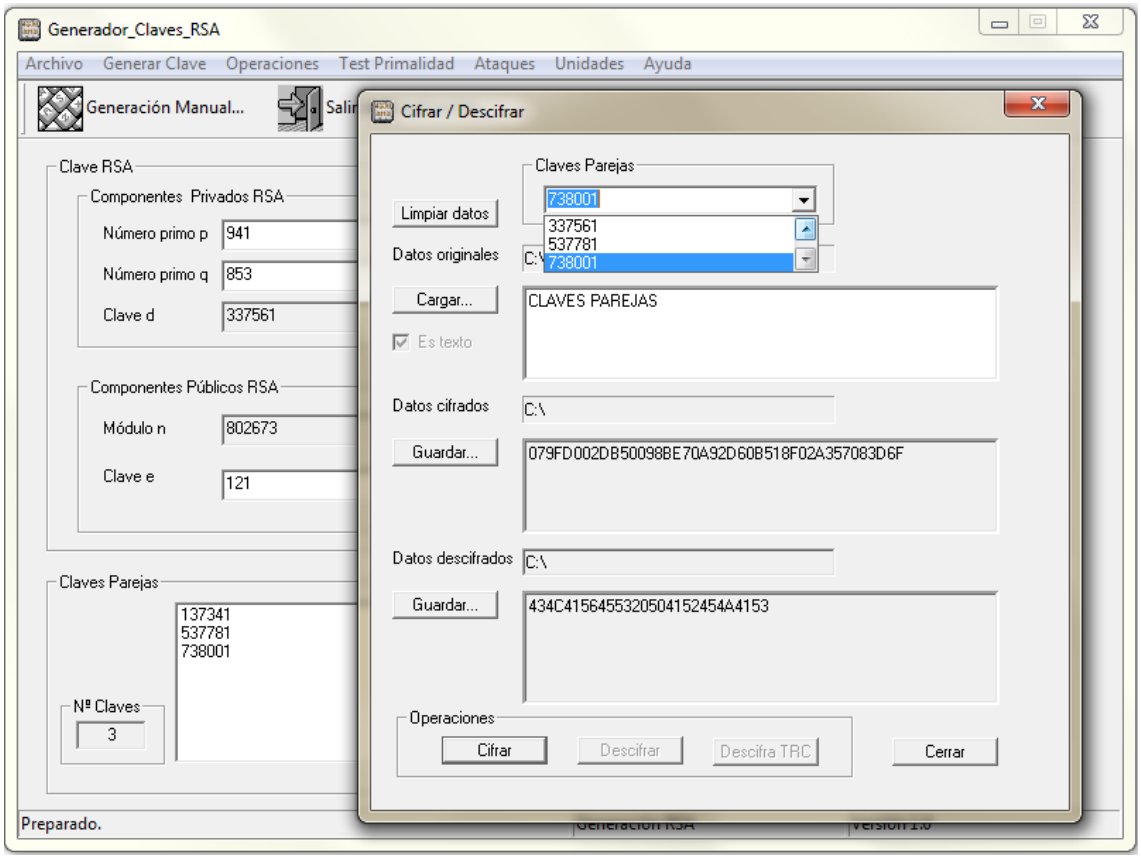
Como ya sabes, ten cuidado al copiar y pegar números muy grandes desde PDF debido al error que comete este programa al dejar fuera el último elemento.

ejercicioRSA4.1.1

Sin contar con la ayuda de ningún software, excepto una calculadora, y usando las ecuaciones que se han mostrado en la diapositiva y que también están en el PDF de la lección y del curso, encuentra la cantidad y los valores de las claves privadas parejas de esta clave RSA de 20 bits:

Clave RSA: p = 941, q = 853, e = 121.

Hecho esto, comprueba con el software genRSA que se descifra el criptograma con cualquiera de las claves privadas.
SW genRSA: http://www.criptored.upm.es/software/sw_m001d.htm



LECCIÓN 4. CLAVES PRIVADAS Y PÚBLICAS PAREJAS

Apartado 4.2. Minimizando las claves privadas parejas

prácticaRSA4.2.1

Con el software genRSA o con ExpoCrip genera estas claves RSA con primos seguros y no seguros y observa cómo se comportan las claves privadas parejas. Observa que genRSA genera claves mayores que 32 bits sólo en formato hexadecimal y ExpoCrip sólo en formato decimal.
SW genRSA: http://www.criptored.upm.es/software/sw_m001d.htm
SW ExpoCrip: http://www.criptored.upm.es/software/sw_m001l.htm
SW dec4hex: http://www.criptored.upm.es/software/sw_m051b.htm
SW Fortaleza de Cifrados: http://www.criptored.upm.es/software/sw_m001e.htm

Generación de claves RSA decimales con primos seguros y no seguros:
Clave 1. p = 43, q = 97, e = 13
Clave 2. p = 47, q = 83, e = 13
Clave 3. p = 7321, q = 2011, e = 101
Clave 4. p = 3037, q = 3433, e = 4111
Clave 5. p = 3023, q = 6599, e = 101
Clave 6. p = 10177, q = 79903, e = 331
Clave 7. p = 468623, q = 2003, e = 349
Clave 8. p = 10007, q = 87383, e = 331
Clave 9. p = p = 59771, q = 50159, e = 33
Clave 10. p = 27376117, q = 27487849, e = 559
Clave 11. p = 992419357, q = 948590171, e = 15187
¿Cuáles de estas claves en decimal usan primos seguros? Comprueba que lo son.

Generación de claves RSA hexadecimales con primos seguros y no seguros:
Clave 1. p = F7223, q = E907B, e = 1DD5
Clave 2. p = 397F27B60D, q = 3DFB19D365, e = 1081
Clave 3. p = 3BD4F0F46ED0F, q = 0346C2CB14BB4B, e = 7369
Clave 4. p = CE20905B95429861, q = D22A5210A721E341, e = 4A23
Clave 5. p = D500DEB29AA95737, q = EDD8937CA8DEBCA7, e = 2E97
Clave 6. e = 2AC5
p = F7C24FAD73B3AD3B0E51BE86F2946969E045240FA510BAACF9DA4B6AA6559523
q = D91C96EA58BDB7BA8988765D44A95FF8AEFDEFE83C74614C26BAC5C3191652CF
¿Cuáles de estas claves en hexadecimal usan primos seguros? Comprueba que lo son.

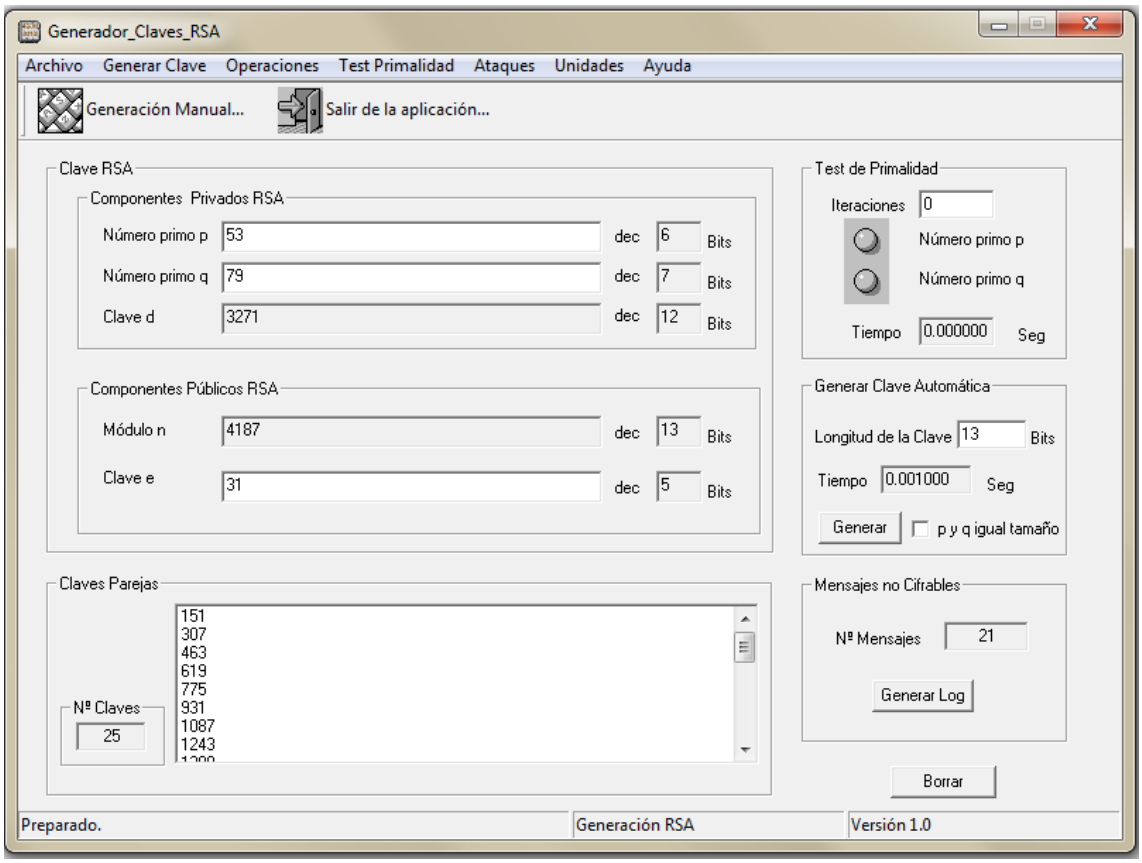
prácticaRSA4.2.2

Con el software genRSA encuentra todas las claves RSA posibles para los primos dados p = 53, q = 79, en función de la clave pública elegida e desde su valor más pequeño posible hasta un número menor que 100.

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

Como n = 53 x 79 = 4.187 y $\phi(n) = (53-1)(79-1) = 4.056 = 2^3 \times 3 \times 13^2$, los valores posibles de la clave pública e menores que 100 serán: 5, 7, 11, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 67, 71, 73, 77, 79, 83, 85, 89, 95, 97.

Genera todas estas claves y observa los valores de las claves privadas parejas. Qué otras claves públicas e entregan 25 CPP?



prácticaRSA4.2.3

Con el software genRSA comprueba que la elección de primos seguros no es sinónimo de generación de claves con una sola CPPP, si bien su valor siempre será muy bajo.

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

Genera una clave RSA con los primos seguros p = 11, q = 47 y los siguientes valores de la clave pública e:

e = 3, 7, 9, 11, 13, 17, 19, 21, 27, 29, 31, 33, 37, 39, 41, 43, 47 y 49.

¿Todas las claves han salido con una sola clave privada pareja?

prácticaRSA4.2.4

Con el software genRSA genera estas 7 claves que tienen como características común entregar un valor alto de claves privadas parejas.

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

Clave 1 de 40 bits: p = EC34D, q = D0099, e = 392F

Clave 2 de 50 bits: p = 175B67F, q = 1B1E30D, e = 7A53

Clave 3 de 60 bits: p = 350A0031, q = 3F5BDC71, e = 4115

Clave 4 de 70 bits: p = 721142905, q = 74FEE9CF1, e = 426B

Clave 5 de 80 bits: p = FAC8541789, q = EA93F345AD, e = 5801

Clave 6 de 90 bits: p = 1E6C319C9C61, q = 19FE6BD6EE21, e = 7411

Clave 7 de 100 bits: p = 331C74A4BDB09, q = 3D4E8FA794B99, e = 443F

LECCIÓN 4. CLAVES PRIVADAS Y PÚBLICAS PAREJAS

Apartado 4.3. También existirán claves públicas parejas

ejercicioRSA4.3.1

A continuación se muestran dos ecuaciones que corresponden a cifras con RSA:

$5.266^{131} \bmod 78.119$

$1.075^{50.891} \bmod 78.119$

Sólo usando los conceptos los conceptos de clave pública, clave privada e inversos en un cuerpo vistos en el curso, ¿cuál de ellas podría ser la de cifra para un intercambio seguro de clave y cuál la de una firma digital?

Puesto que el cuerpo de cifra 78.119 es el mismo en ambos casos, cabría esperar que se trata de dos operaciones con la misma clave RSA, una con la clave pública y otra con la clave privada. Como ya hemos comentado en lecciones anteriores, lo normal es que la clave pública sea mucho menor que la clave privada; por tanto vamos a suponer que 131 es la clave pública y que 50.891 debería ser su correspondiente clave privada.

Comprobación:

Si n = 78.119, factorizamos este número con el software ExpoCrip o factor y encontramos que p = 191 y q = 409. Luego, $\phi(n) = (p - 1)(q - 1) = 190 \times 408 = 77.520$ y debería cumplirse que la clave pública y la privada fuesen inversas en $\phi(n)$. Si eso es verdad, entonces se cumplirá la relación $e \times d = k\,\phi(n) + q$, esto es que $131 \times 50.891 = 6.666.721 = k \times 77.520 + 1$.
Esto es cierto para k = 86.

Concluimos que la clave pública e será 131 y la clave privada d será 50.891. En el primer caso habremos cifrado confidencialmente el número secreto 5.266 y en el segundo caso habremos firmado digitalmente el número 1.075.

LECCIÓN 4. CLAVES PRIVADAS Y PÚBLICAS PAREJAS

Apartado 4.4. ¿Hay que preocuparse por estas claves parejas?

prácticaRSA4.4.1

Con el software genRSA genera esta clave RSA.

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

p =
6599B440F8EB2EC0EAFB875A71ADE32F764D2E0AE92361961C4800CF69B8E7B71BA7474A8C19ECB38AADC1C0FFB99594D19C1F9C085040C42F3F89EAFC58FD9371
q =
17A081626BD565D0544917C77BB01EB28F1CA926EB01C2F2042ABF7AB335F8062594CDE1612E40DE7CD6B8F59CCAC55AB28EBE364151AB02E6750CBE75576F3
e = 7A2D

Una vez generada, guárdala con el nombre de Clave1024_3149CPP.html.
Para saber el tamaño en bits de la clave privada pareja más pequeña, abre ese archivo html, copia al portapapeles la primera clave pareja que aparece y la pegas como si fuese un primo p de una nueva clave. Repite lo mismo ahora con la última clave pareja que aparece en ese archivo html y la pegas como si fuese el primo q.
Aquí lo que buscamos es que el mismo programa genRSA nos indique el tamaño de cada una de estas dos claves.

¿Comprueba que aunque son muchas CPP todos sus valores son inmensos y, por tanto, seguros ante un ataque por fuerza bruta