Proyecto CLCript
Cuadernos de Laboratorio de Criptografía. Entrega nº 5. Última actualización 06/05/19
Autor: Dr. Jorge Ramió Aguirre (@criptored)
Prácticas con el algoritmo RSA: claves parejas

- Software genRSA v2.1: http://www.criptored.upm.es/software/sw_m001d.htm
- Software SAMCript: http://www.criptored.upm.es/software/sw_m001t.htm
- Lectura de interés: http://www.criptored.upm.es/crypt4you/temas/RSA/leccion4/leccion04.html
- Lectura de interés: https://en.wikipedia.org/wiki/Safe_prime

Objetivos:

1. Observar las claves privadas parejas y las claves públicas parejas de una clave RSA.
2. Comprobar que dichas claves realizan la misma función que sus claves directas.
3. Comprobar que este fenómeno no se traduce en una vulnerabilidad en RSA.
4. Comprobar que con el uso de primos seguros se minimiza la cantidad de estas claves parejas.
5. Comprobar que las claves privadas parejas se generan al formarse anillos en la operación de cifra. Observar además que, en función del número secreto que se vaya a cifrar, pueden formarse anillos de cifra más pequeños donde aparecen nuevos números que realizan la misma función que la clave privada o que una clave privada pareja, sin ser éstos.

I. Claves privadas parejas en RSA

Ejercicio 1)

1.1. Con genRSA v2.1 genera de forma Manual una clave RSA con p = 31, q = 101, e = 7.

1.2. Observa que se obtienen 10 claves privadas parejas CPP y que la separación entre ellas es el valor 300 como se aprecia: 43, 343, 643, 943, 1.243, 1.543, 1.843, 2.443, 2.743, 3.043, excepto en la zona donde se encuentra la clave privada 2.143.

1.3. Comprueba con genRSA v2.1 que en Operaciones al cifrar el valor 2.145 se obtiene el criptograma 2.238 y que al descifrarlo con cualquiera de esas claves privadas, se recupera el mensaje original 2.145.

1.4. Comprueba una de estas operaciones con la calculadora de Windows.

1.5. Genera de forma Automática, con p y q de igual tamaño y e = 65.537 (no actives primos seguros) varias claves de 1.024 bits en decimal, hasta obtener una con más de 40 CPP.

1.6. Observa el tamaño de esas claves privadas parejas (ordenadas de menor a mayor), usando el *scrollbar* horizontal y vertical de esa ventana.

1.7. Cambia las Unidades a hexadecimal y genera de forma Manual esta clave con e = 10001:
p = BEC96D795ADE4CC6FAA73676E43EB08867C81C6C864938729FBDE9834A64370F845D98460D76718B0E43DA25FF6DA238C84D92F426B9F60D511E5A6BDCCF92E1
q = F25CB470A2CF2CD35756E7F72D4BE5AB48918A92527AF42371E88CF376B3DB37584BA084E09F1FDAA53DBBE13BBAC772A8549A5917D6E15AD1BC3A726898FFEF

1.8. Observa la cantidad de CPP que se obtienen y vuelve a usar el *scrollbar*. Guarda esta clave como clave1024_muchasCPP.html.

1.9. Aunque la clave RSA anterior sea de 1.024 bits y hoy se usen claves de 2.048 bits, ¿podría ser ésta una clave real de un servidor web seguro de hace unos 5 o más años?

1.10. Abre el archivo clave1024_muchasCPP.html y comprueba que la clave privada pareja de menor tamaño tiene 1.011 bits y la mayor 1.024 bits.

1.11. ¿Por qué motivo todas las CPP se encuentran tan cerca del módulo de cifra?
1.12. ¿El hecho de que esta clave tenga más de 3.600 CPP, la convierte en débil? ¿Por qué sí o por qué no? Justifica tu respuesta.
1.13. Genera de forma Automática en hexadecimal una clave RSA de 2.048 bits real, con Clave pública e = 10001, p y q de 1.024 bits (sin primos seguros), y que tenga más de 50 CPP.
1.14. En un próximo cuaderno de laboratorio vamos a generar claves RSA con OpenSSL y vas a comprobar que ese programa no muestra las CPP. ¿Por qué crees que no las muestra?

Comprueba tu trabajo:

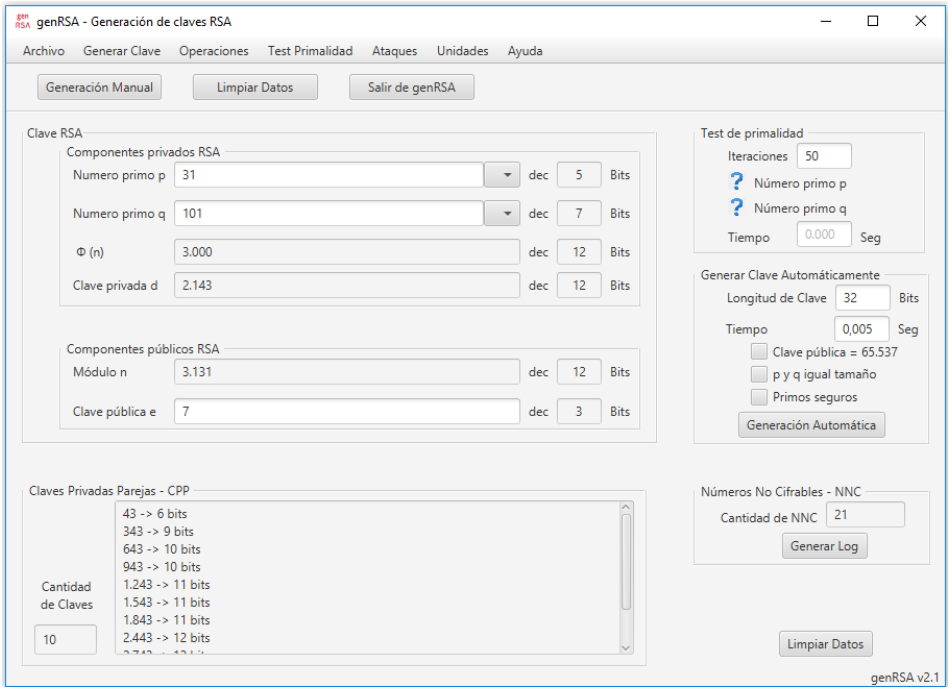

Figura 1. Clave RSA de 12 bits

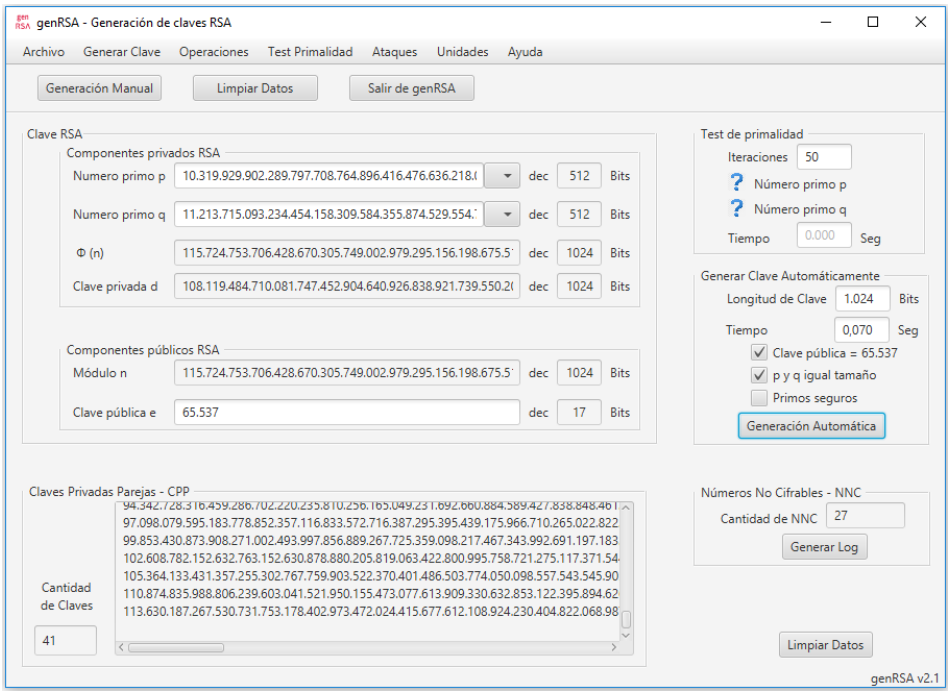

Figura 2. Clave RSA de 1.024 bits decimal.

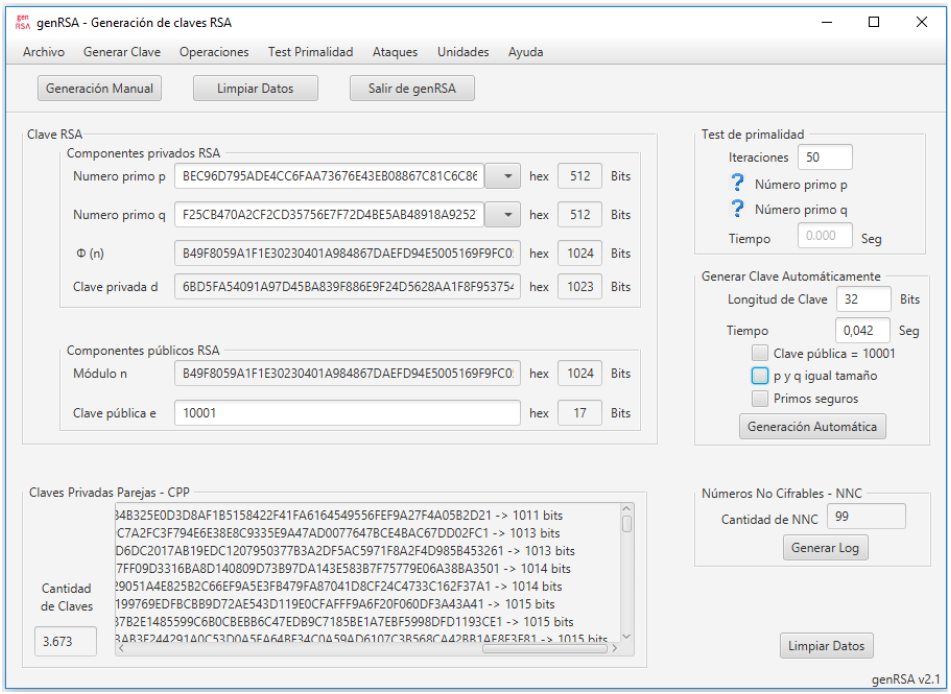

Figura 3. Clave RSA de 1.024 bits hexadecimal.

.

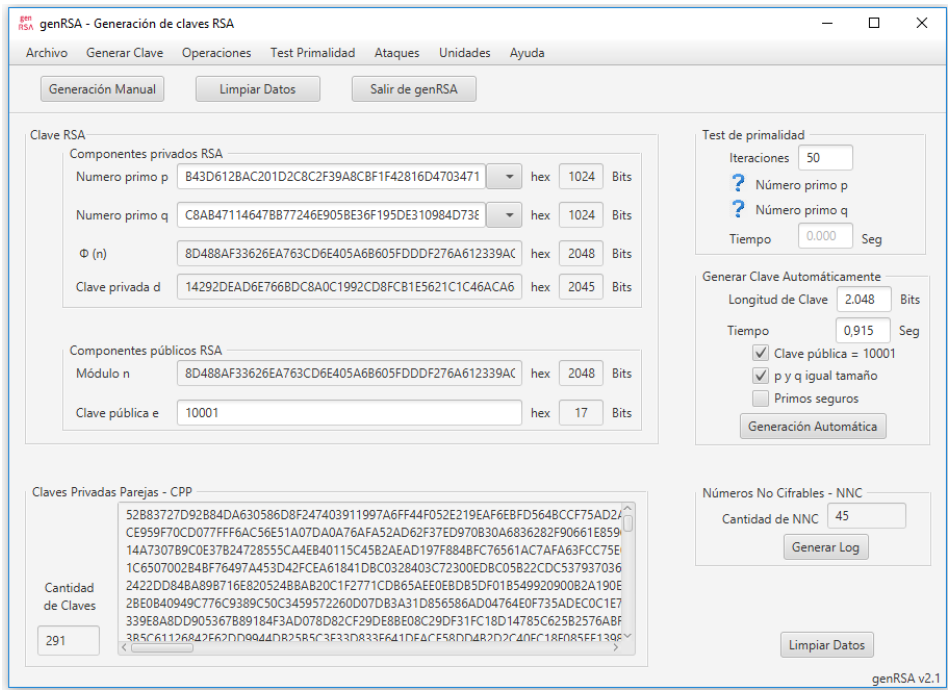

Figura 4. Clave RSA de 2.048 bits hexadecimal.

II. Minimizando las claves privadas parejas en RSA

Ejercicio 2)

2.1. Con genRSA v2.1 genera de forma Manual una clave RSA decimal eligiendo desde la misma ventana los valores de p y q como primos de 3 dígitos y pon como clave pública un número impar de 2 dígitos, e.g. 11, 37, 49, 63, etc.

2.2. Como los valores que propone genRSA v2.1 son primos seguros, comprueba que la cantidad de CPP siempre será 1, la menor posible.

2.3. Genera de forma Automática varias claves de 300 bits, desactivando todas las opciones de la Generación Automática.

2.4. Comprueba que en este caso el valor de Clave pública e será siempre el número impar más bajo posible y que el número de CPP cambia de una a otra clave.

2.5. ¿Por qué siempre la clave pública, o la clave privada, es un número impar? ¿Por qué no puede ser un número par?

2.6. Repite el apartado 2.3 activando ahora solamente la opción Primos seguros.

Comprueba tu trabajo:

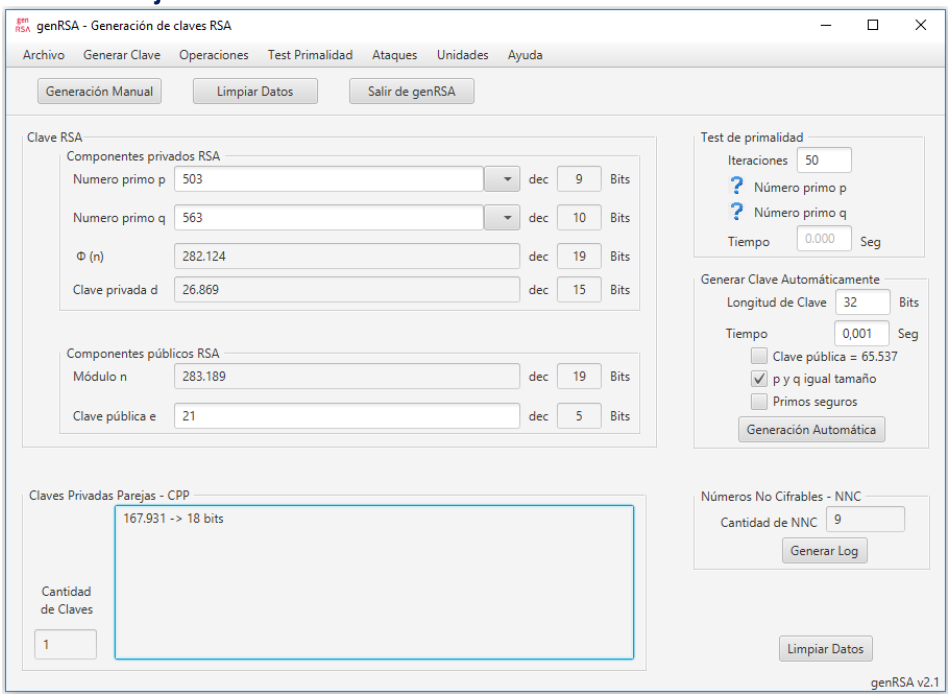

Figura 5. Clave RSA de 19 bits.

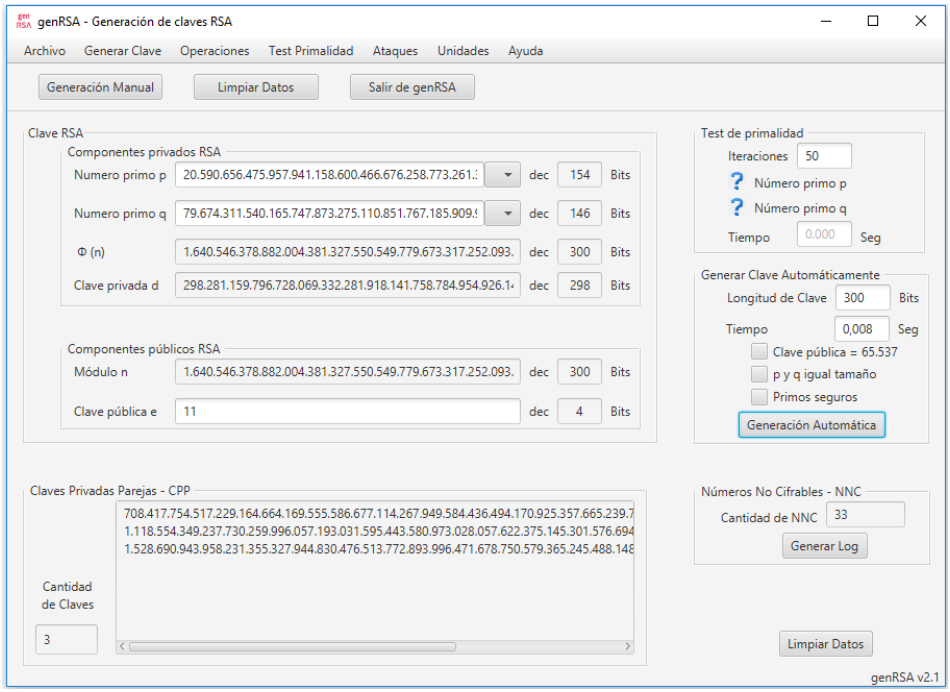

Figura 6. Clave RSA de 300 bits.

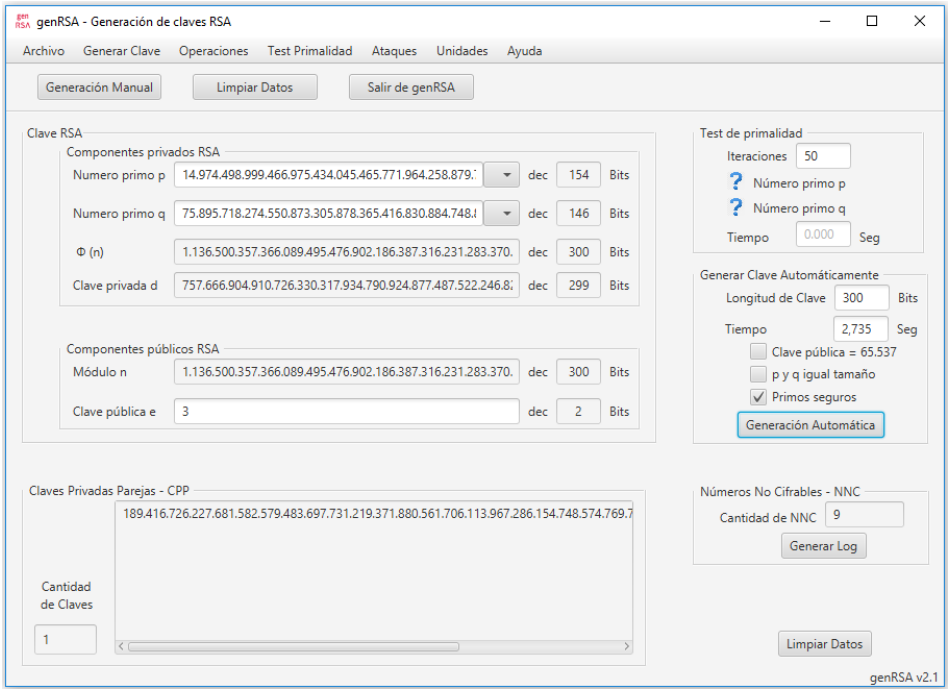

Figura 7. Clave RSA de 300 bits con primos seguros.

III. Los primos seguros no garantizan CPP = 1

Ejercicio 3)

3.1. Genera de forma Manual una clave RSA decimal de 8 bits con p = 7, q = 23, ambos primos seguros (7 = 2x3 + 1 y 23 = 2x11 + 1) y e = 5, el menor posible. Observa que el número de claves privadas parejas es 1.

3.2. Usa ahora e = 7, 19, 23, 35, 37, 53. Observa que a pesar de usar primos seguros, no obtenemos el número mínimo de CPP, aunque sí un valor muy bajo, 2.

Comprueba tu trabajo:

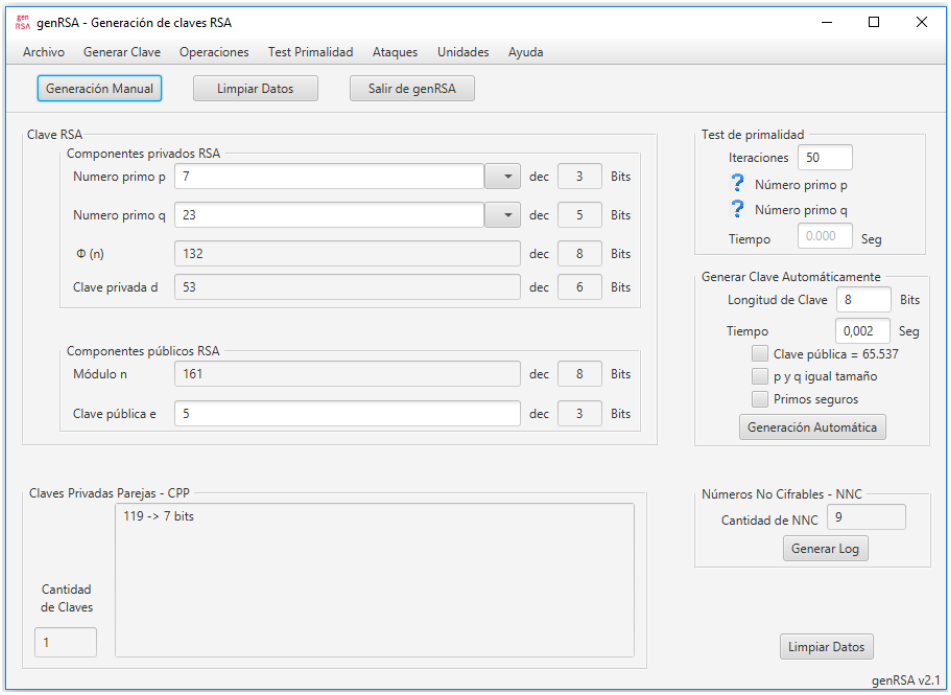

Figura 8. Clave RSA con primos seguros p = 7, q = 23 y e = 5 (1 CPP)

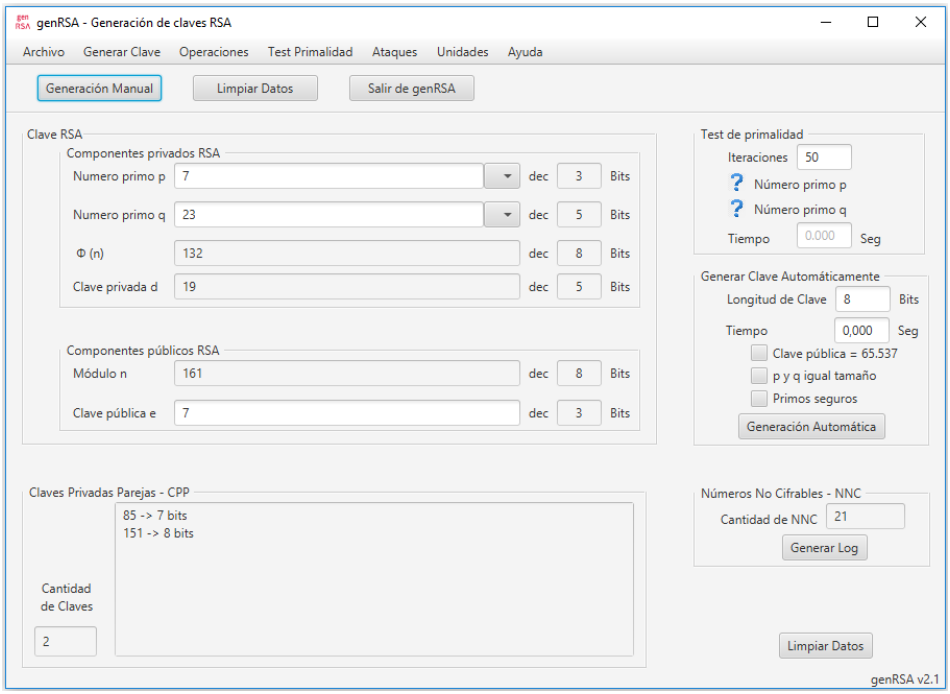

Figura 9. Clave RSA con primos seguros p = 7, q = 23 y e = 7 (2 CPP)

IV. Claves públicas parejas en RSA

Ejercicio 4)

4.1. Genera de forma Manual una clave RSA decimal con p = 2.441, q = 3.769, e = 65.537.

4.2. Copia al portapapeles el valor de la clave privada 6.678.593 y pega ese valor en la casilla de la Clave pública e. Hecho esto, haz clic en Generación Manual.

4.3. Observa que las claves pública y privada han cambiado de lugar. Los números que se observan ahora como “Claves Privadas Parejas”, corresponderán lógicamente a las Claves Públicas Parejas.

4.4. Repite el ejercicio, ahora generando de forma Automática varias claves reales en formato hexadecimal de 2.048 bits, con primos p y q de igual tamaño y Clave pública 10001, hasta que tengas una clave con solo 1 Clave Privada Pareja.

4.5. Selecciona el valor de la Clave privada d y cópiala en el portapapeles. Pega ese número en la casilla de la Clave pública e.

4.6. Hecho esto, vuelva generar la clave pero ahora Manualmente y observa lo que sucede con las claves pública y privada.

4.7. Observa que en muchos casos, la cantidad de Claves Públicas Parejas aumenta en una unidad con respecto a las Claves Privadas Parejas.

4.8. ¿Podría ser un problema el hecho de que se pueda comprobar una firma digital RSA con un valor de clave pública diferente al estándar, el número 4 de Fermat?

4.9. Visto lo anterior, ¿puedes justificar por qué no se permite que el usuario elija un valor aleatorio de clave pública?

4.10. Si se permitiese que el usuario al generar su clave RSA pudiera elegir un valor aleatorio para su Clave pública, ¿qué limitaciones le pondrías?

Comprueba tu trabajo:

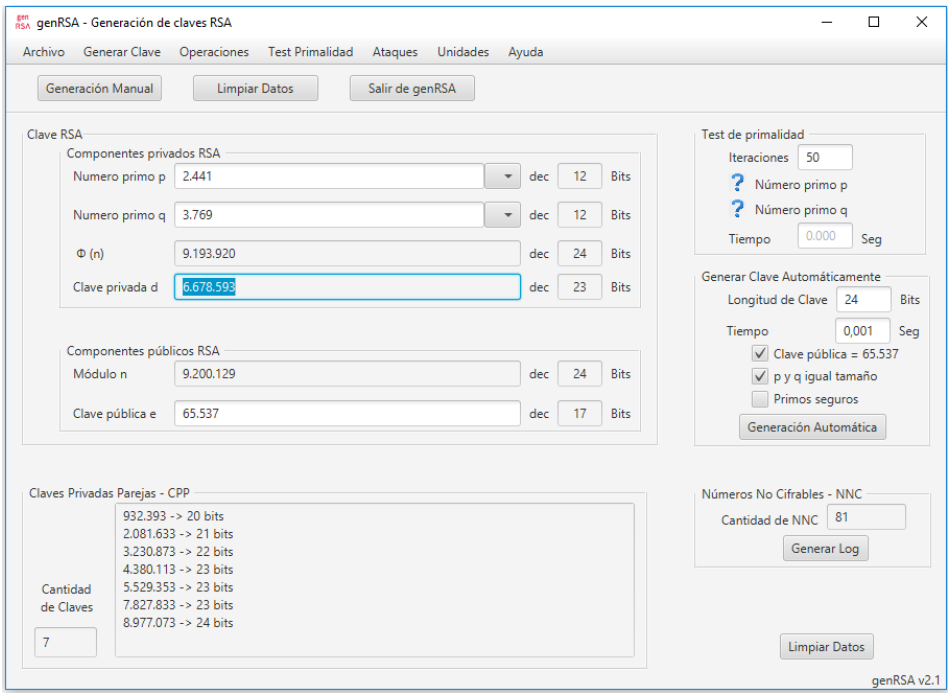

Figura 10. Generación de una clave RSA de 24 bits con e = F4.

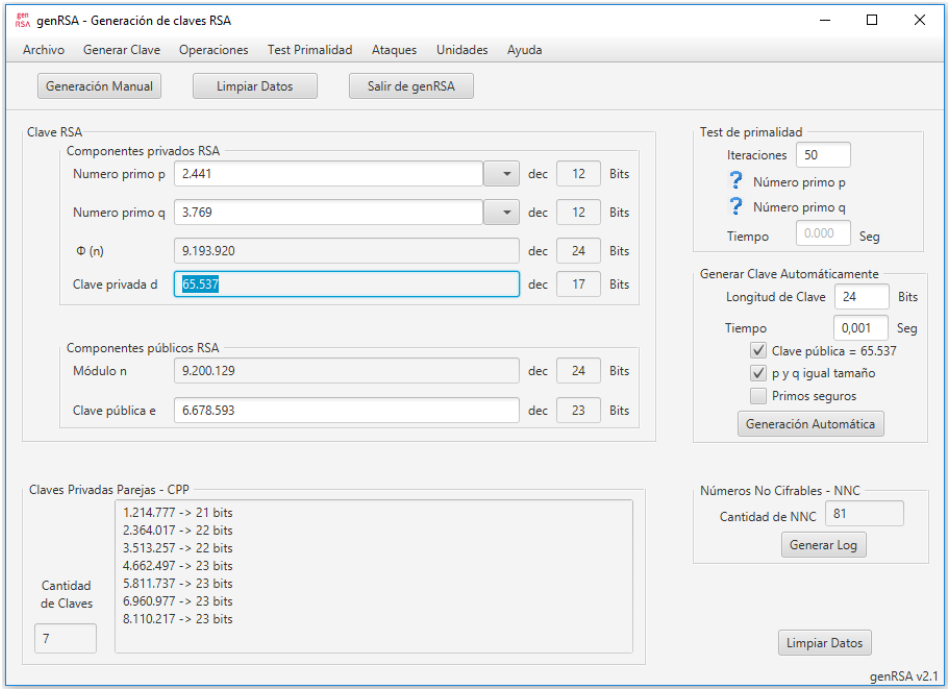

Figura 11. Misma clave de la figura 7 pero generándola otra vez introduciendo como clave pública e el valor encontrado para la clave privada d. Objetivo: observar las claves Públicas Parejas de una clave RSA de 24 bits.

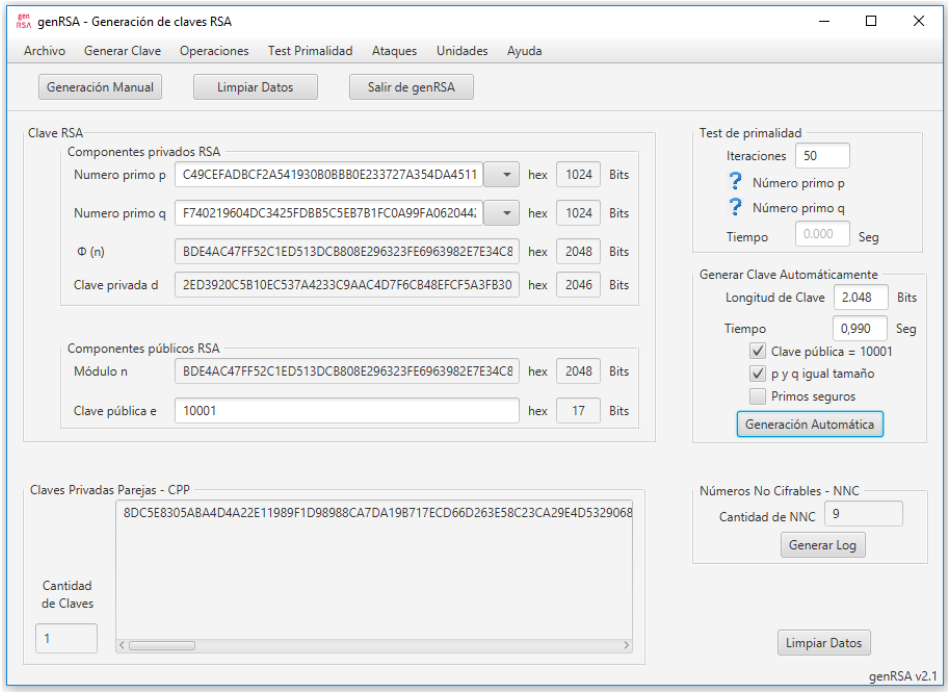

Figura 12. Generación de una clave RSA de 2.048 bits en hexadecimal 24 bits con e = 10001.

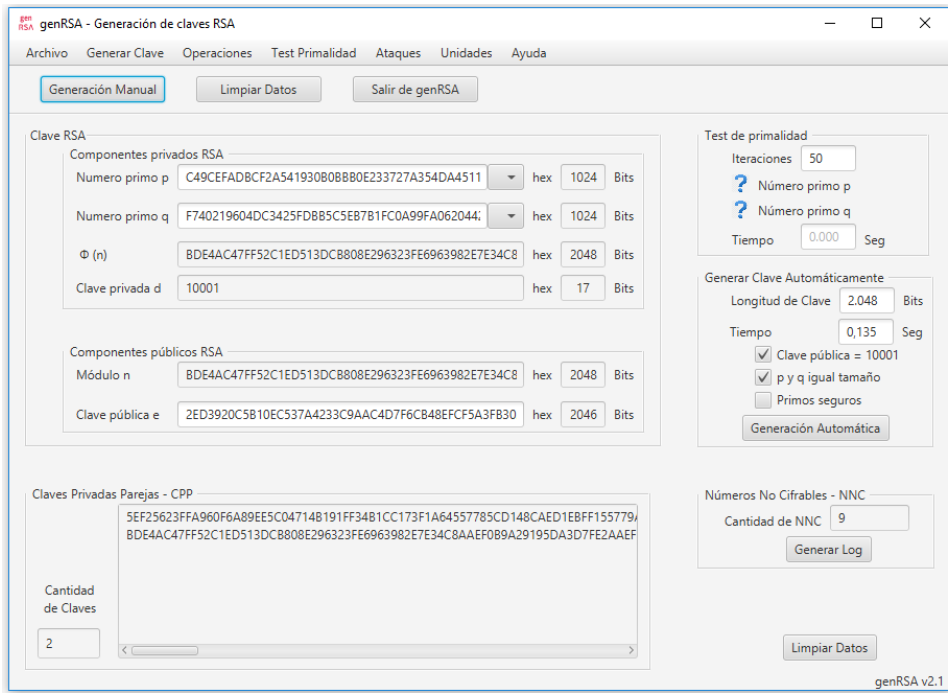

Figura 13. Misma clave de la figura 9 pero generándola otra vez introduciendo como clave pública e el valor encontrado para la clave privada d. Objetivo: observar las claves Públicas Parejas de una clave RSA de 2.048 bits.

V. Generación de anillos en la cifra RSA y nuevas claves válidas

Ejercicio 5)

5.1. Con genRSA v2.1 genera de forma Manual la clave RSA en decimal: p = 7, q = 11, e = 13.

5.2. Comprueba que la clave privada d = 37 y que hay dos claves privada parejas 7 y 67.

5.3. Comprueba con genRSA v2.1 que el secreto 2 se cifra como 30.

5.4. Con SAMCript descifra el criptograma 30 del apartado anterior con todos los restos del módulo 77 {0, …, 76} y observa que sólo se recupera el secreto 2 con la clave privada y las claves privadas parejas.

5.5. Observa el anillo de longitud 30 que se forma en el descifrado.

Comprueba tu trabajo:

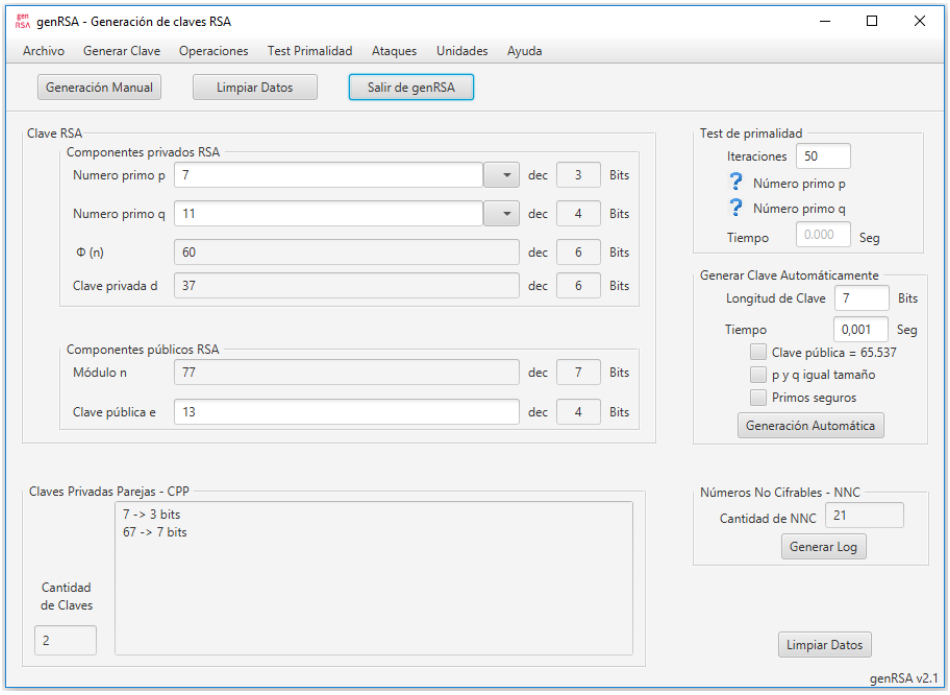

Figura 14. Clave con p = 7, q = 11, e = 13.

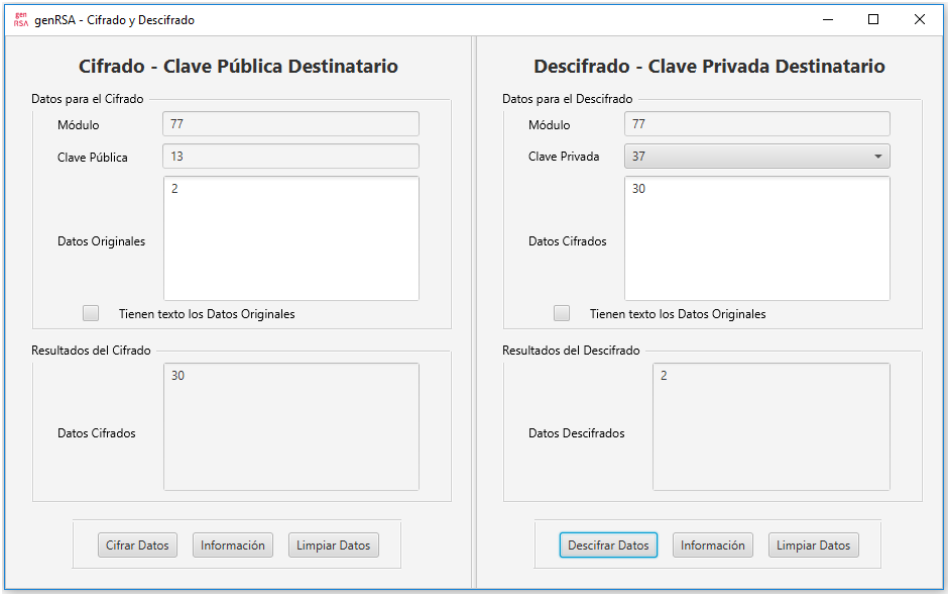

Figura 15. Cifrado del número secreto 2 y su descifrado.

Clave RSA1: p = 7, q = 11, n = 77, $\phi(n) = 60$, e = 13, d = 37 y CPP: d1 = 7, d2 = 67 Número a cifrar N = **2** $C^e \bmod n = 2^{13} \bmod 77 =$ **30**				
Con N = 2 se cumple que sólo se descifra con d y con las CPP				
$30^0 \bmod 77 = 1$	$30^1 \bmod 77 = 30$	$30^2 \bmod 77 = 53$	$30^3 \bmod 77 = 50$	$30^4 \bmod 77 = 37$
$30^5 \bmod 77 = 32$	$30^6 \bmod 77 = 36$	$30^7 \bmod 77 = 2$	$30^8 \bmod 77 = 60$	$30^9 \bmod 77 = 29$
$30^{10} \bmod 77 = 23$	$30^{11} \bmod 77 = 74$	$30^{12} \bmod 77 = 64$	$30^{13} \bmod 77 = 72$	$30^{14} \bmod 77 = 4$

$30^{15} \bmod 77 = 43$	$30^{16} \bmod 77 = 58$	$30^{17} \bmod 77 = 46$	$30^{18} \bmod 77 = 71$	$30^{19} \bmod 77 = 51$
$30^{20} \bmod 77 = 67$	$30^{21} \bmod 77 = 8$	$30^{22} \bmod 77 = 9$	$30^{23} \bmod 77 = 39$	$30^{24} \bmod 77 = 15$
$30^{25} \bmod 77 = 65$	$30^{26} \bmod 77 = 25$	$30^{27} \bmod 77 = 57$	$30^{28} \bmod 77 = 16$	$30^{29} \bmod 77 = 18$
$30^{30} \bmod 77 = 1$	$30^{31} \bmod 77 = 30$	$30^{32} \bmod 77 = 53$	$30^{33} \bmod 77 = 50$	$30^{34} \bmod 77 = 37$
$30^{35} \bmod 77 = 32$	$30^{36} \bmod 77 = 36$	$30^{37} \bmod 77 = 2$	$30^{38} \bmod 77 = 60$	$30^{39} \bmod 77 = 29$
$30^{40} \bmod 77 = 23$	$30^{41} \bmod 77 = 74$	$30^{42} \bmod 77 = 64$	$30^{43} \bmod 77 = 72$	$30^{44} \bmod 77 = 4$
$30^{45} \bmod 77 = 43$	$30^{46} \bmod 77 = 58$	$30^{47} \bmod 77 = 46$	$30^{48} \bmod 77 = 71$	$30^{49} \bmod 77 = 51$
$30^{50} \bmod 77 = 67$	$30^{51} \bmod 77 = 8$	$30^{52} \bmod 77 = 9$	$30^{53} \bmod 77 = 39$	$30^{54} \bmod 77 = 15$
$30^{55} \bmod 77 = 65$	$30^{56} \bmod 77 = 25$	$30^{57} \bmod 77 = 57$	$30^{58} \bmod 77 = 16$	$30^{59} \bmod 77 = 18$
$30^{60} \bmod 77 = 1$	$30^{61} \bmod 77 = 30$	$30^{62} \bmod 77 = 53$	$30^{63} \bmod 77 = 50$	$30^{64} \bmod 77 = 37$
$30^{65} \bmod 77 = 32$	$30^{66} \bmod 77 = 36$	$30^{67} \bmod 77 = 2$	$30^{68} \bmod 77 = 60$	$30^{69} \bmod 77 = 29$
$30^{70} \bmod 77 = 23$	$30^{71} \bmod 77 = 74$	$30^{72} \bmod 77 = 64$	$30^{73} \bmod 77 = 72$	$30^{74} \bmod 77 = 4$
$30^{75} \bmod 77 = 43$	$30^{76} \bmod 77 = 58$	Anillos de longitud 30		

Figura 16. Cifrado del número secreto 2 y su descifrado sólo posible con la clave privada d = 37 o las claves privadas parejas 7 y 67 (verde). Anillos de longitud 30.

5.6. Ahora cifra con genRSA v2.1 el secreto 13 y comprueba que se cifra como 41.

5.7. Con SAMCript descifra el criptograma 41 del apartado anterior con todos los restos del módulo 77 {0, …, 76} y observa que, además de la clave privada y de las claves privadas parejas, existen otros números -hasta ahora desconocidos- que también descifran el criptograma y devuelven el secreto 13.

5.8. ¿Qué conclusiones puedes sacar de lo visto?

Comprueba tu trabajo:

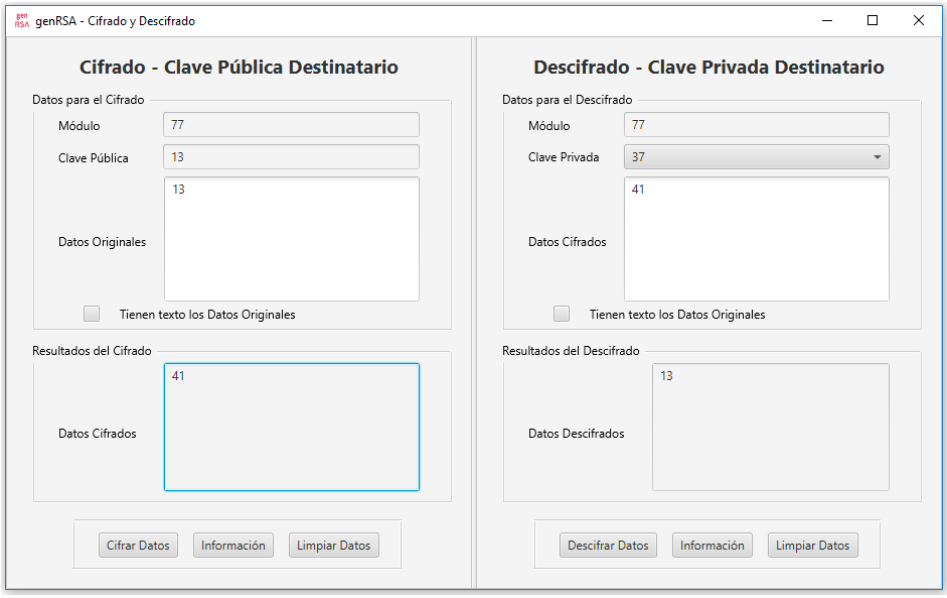

Figura 17. Cifrado del número secreto 13 y su descifrado.

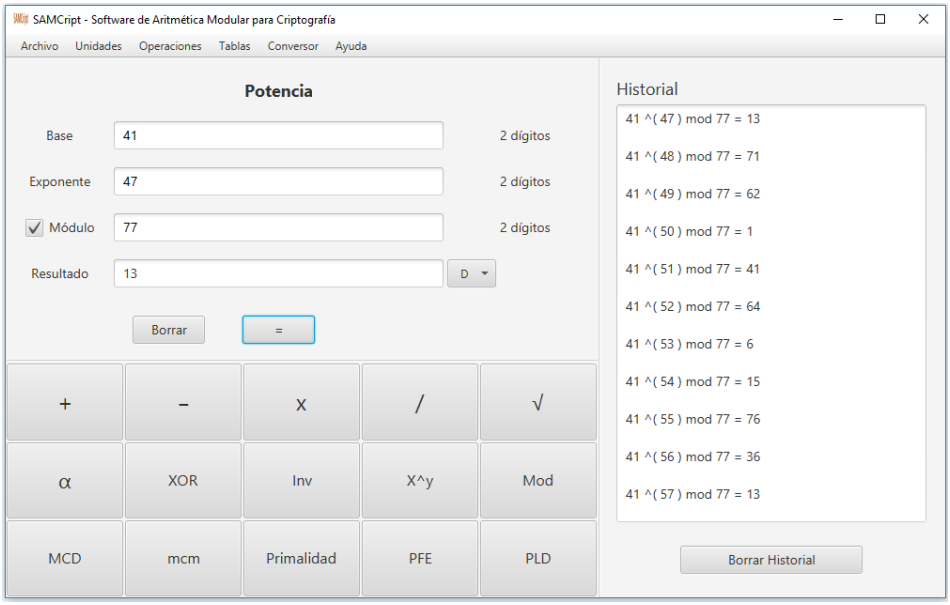

Figura 18. Anillo de longitud 10, en el que se recupera el secreto 13 cifrado con la clave pública e = 13 pero con los números 47 y 57, distintos a la clave privada d = 37 o las claves privadas parejas 7 y 67.

Clave RSA2: p = 7, q = 11, n = 77, $\phi(n)$ = 60, e = 13, d = 37 y CPP: d1 = 7, d2 = 67 Número a cifrar: **13** C^e mod n = 13^{13} mod 77 = **41**				
Con N = 13 NO se cumple que sólo se descifra con d y con las CPP				
41^0 mod 77 = 1	41^1 mod 77 = 41	41^2 mod 77 = 64	41^3 mod 77 = 6	41^4 mod 77 = 15
41^5 mod 77 = 76	41^6 mod 77 = 36	41^7 mod 77 = 13	41^8 mod 77 = 71	41^9 mod 77 = 62
41^{10} mod 77 = 1	41^{11} mod 77 = 41	41^{12} mod 77 = 64	41^{13} mod 77 = 6	41^{14} mod 77 = 15
41^{15} mod 77 = 76	41^{16} mod 77 = 36	41^{17} mod 77 = 13	41^{18} mod 77 = 71	41^{19} mod 77 = 62
41^{20} mod 77 = 1	41^{21} mod 77 = 41	41^{22} mod 77 = 64	41^{23} mod 77 = 6	41^{24} mod 77 = 15
41^{25} mod 77 = 76	41^{26} mod 77 = 36	41^{27} mod 77 = 13	41^{28} mod 77 = 71	41^{29} mod 77 = 62
41^{30} mod 77 = 1	41^{31} mod 77 = 41	41^{32} mod 77 = 64	41^{33} mod 77 = 6	41^{34} mod 77 = 15
41^{35} mod 77 = 76	41^{36} mod 77 = 36	41^{37} mod 77 = 13	41^{38} mod 77 = 71	41^{39} mod 77 = 62
41^{40} mod 77 = 1	41^{41} mod 77 = 41	41^{42} mod 77 = 64	41^{43} mod 77 = 6	41^{44} mod 77 = 15
41^{45} mod 77 = 76	41^{46} mod 77 = 36	41^{47} mod 77 = 13	41^{48} mod 77 = 71	41^{49} mod 77 = 62
41^{50} mod 77 = 1	41^{51} mod 77 = 41	41^{52} mod 77 = 64	41^{53} mod 77 = 6	41^{54} mod 77 = 15
41^{55} mod 77 = 76	41^{56} mod 77 = 36	41^{57} mod 77 = 13	41^{58} mod 77 = 71	41^{59} mod 77 = 62
41^{60} mod 77 = 1	41^{61} mod 77 = 41	41^{62} mod 77 = 64	41^{63} mod 77 = 6	41^{64} mod 77 = 15
41^{65} mod 77 = 76	41^{66} mod 77 = 36	41^{67} mod 77 = 13	41^{68} mod 77 = 71	41^{69} mod 77 = 62
41^{70} mod 77 = 1	41^{71} mod 77 = 41	41^{72} mod 77 = 64	41^{73} mod 77 = 6	41^{74} mod 77 = 15
41^{75} mod 77 = 76	41^{76} mod 77 = 36	Los números 17, 27, 47 y 57 ejercen también como CPP		

Figura 19. Cifrado del número secreto 13 y su descifrado posible con la clave privada d = 37, las claves privadas parejas 7 y 67 y, además, con 17, 27, 47 y 57 (amarillo). Anillos de longitud 10.

Nota:

El hecho de haber usado como secreto el mismo valor de la clave pública (13), no tiene ninguna incidencia.

A igual resultado se llega si se usa otra clave pública, por ejemplo e = 17, con lo que la clave RSA tendrá como clave privada d = 53 y una única clave privada pareja 23.

Cifrando el secreto: C = 13^{17} mod 77 = 62.

El criptograma 62 se descifra con 3, 13, 23, 33, 43, 53, 63 y 73, en anillos de longitud 10, y en donde 3, 13, 33, 43, 63 y 73 son valores no conocidos que ejercen como si fuesen claves privadas parejas.

Recuerdo del cálculo de las claves privadas parejas CPP

REF.: http://www.criptored.upm.es/descarga/CursoCriptografiaAplicada2018.pdf

Sea:

- $\gamma = mcm\ [(p-1), (q-1)]$
- $d_\gamma = e^{-1} \bmod \gamma = inv\ (e, \gamma)$

Entonces, la clave privada d tendrá λ claves parejas d_i de la forma:

- $d_i = d_\gamma + i\ \gamma \qquad 1 < d_i < n$
- $i = 0, 1, \ldots \lambda \qquad \lambda = \lfloor (n - d_\gamma)/\gamma \rfloor$

En el ejercicio con p = 7, q = 11, n = 77, e = 13, tenemos:

- $\gamma = mcm\ [(p-1), (q-1)] = mcm\ (6, 10) = 30$
- $d_\gamma = inv\ (13, 30) = 7$
- $\lambda = \lfloor (n - d_\gamma)/\gamma \rfloor = \lfloor (77 - 7)/30) \rfloor = \lfloor 70/30 \rfloor = \lfloor 2{,}33 \rfloor = 2$
- $d_i = d_\gamma + i\ \gamma = 37 + i*30$ con i = 0, 1, 2
  - i = 0 $d_1 = 7$
  - i = 1 $d_2 = 37$
  - i = 2 $d_3 = 67$
- Siendo $d_2 = d = 37$ la clave privada puesto que $d = inv\ (e, \phi(n)) = inv\ (13, 60) = 37$

Puedes utilizar esta documentación, otros libros, material multimedia y software de prácticas generados en Criptored, todos de libre distribución en Internet, para poder demostrar que entiendes y sabes cómo trabaja la criptografía, logrando la nueva certificación técnica profesional CriptoCert Certified Crypto Analyst, reconocida por el Centro Criptológico Nacional CCN de España, disponible desde el mes de abril de 2019.

Encontrarás más información sobre esta certificación y correo de contacto en el sitio web: https://www.criptocert.com

Madrid, 6 de mayo de 2019

Dr. Jorge Ramió Aguirre