



CRYPT4YOU

DOCUMENTO ANEXO A LA LECCIÓN 5

DEL CURSO "EL ALGORITMO RSA"

EJERCICIOS Y PRÁCTICAS PROPUESTOS Y RESUELTOS

Autor: Dr. Jorge Ramió Aguirre

Fecha de publicación: 21 de mayo de 2012

<http://www.criptored.upm.es/crypt4you/temas/RSA/leccion5/leccion05.html>

TABLA DE CONTENIDOS

LECCIÓN 5. MENSAJES NO CIFRABLES	2
Apartado 5.1. ¿Qué son los mensajes no cifrables?	2
prácticaRSA5.1.1	2
Apartado 5.2. Calculando los números no cifrables	3
prácticaRSA5.2.1	3
ejercicioRSA5.2.1	4
Apartado 5.3. Minimizando los números no cifrables	5
prácticaRSA5.3.1	5
prácticaRSA5.3.2	6
Apartado 5.4. ¿Hay que preocuparse por estos números no cifrables?	7
prácticaRSA5.4.1	7

LECCIÓN 5. MENSAJES NO CIFRABLES

Apartado 5.1. ¿Qué son los mensajes no cifrables?



prácticaRSA5.1.1

Con el software Fortaleza de Cifrados, comprueba que todos estos números secretos se transmiten en claro al cifrarlos con RSA.

Números sin puntos para que puedas usar la opción de copia y pegar.

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

Clave RSA1 de 16 bits:

$n = 43739$, $e = 103$, $p = 191$, $q = 229$.

Números a cifrar: 19101, 21392, 41448.

Clave RSA2 de 20 bits:

$n = 753041$, $e = 6757$, $p = 739$, $q = 1019$.

Números a cifrar: 164058, 164059, 638914.

Clave RSA3 de 26 bits:

$n = 47142611$, $e = 47$, $p = 6637$, $q = 7103$.

Números a cifrar: 3338411, 43804200, 43804201.

LECCIÓN 5. MENSAJES NO CIFRABLES

Apartado 5.2. Calculando los números no cifrables



prácticaRSA5.2.1

Con el software genRSA y luego con ExpoCrip genera estas 6 claves RSA, apunta la cantidad de mensajes o números no cifrables y encuentra esos valores haciendo la operación que te permite la aplicación. Dado el alto tiempo que toma esta operación para números grandes, solamente se generarán claves de hasta 25 bits.

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

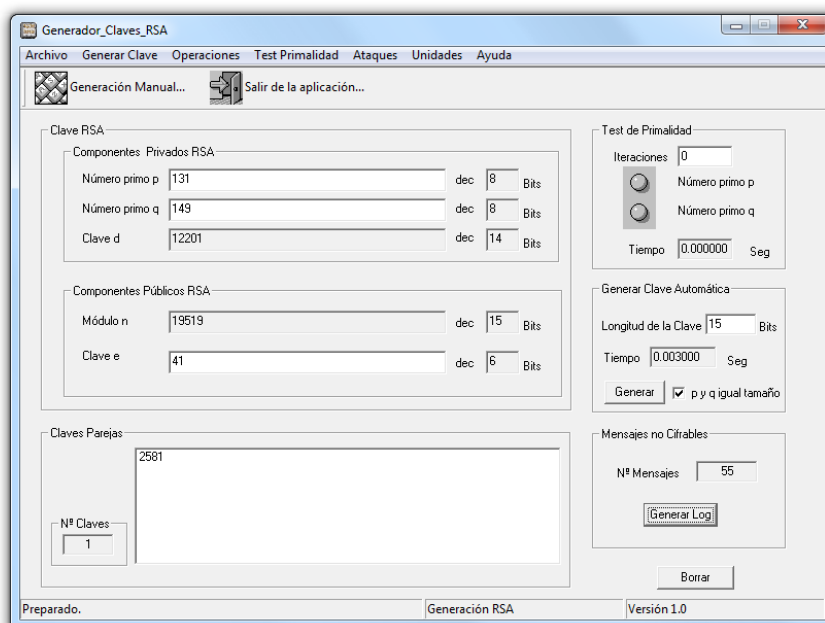
SW ExpoCrip: http://www.criptored.upm.es/software/sw_m001l.htm

- Clave 1 de 8 bits: $p = 13, q = 17, e = 7$
- Clave 2 de 12 bits: $p = 47, q = 59, e = 19$
- Clave 3 de 15 bits: $p = 131, q = 149, e = 41$
- Clave 4 de 18 bits: $p = 409, q = 499, e = 31$
- Clave 5 de 20 bits: $p = 743, q = 991, e = 31$
- Clave 6 de 25 bits: $p = 3061, q = 7603, e = 127$

MENSAJES NO CIFRABLES

El número de Mensajes no cifrables va a ser: 55

0
1
446
597
744
2428
2489
2681
3726
4322
4365
4663
4769
4917
5067
5110
5706
6854
7004
7152
7406
7598
7599
8195
8835
9343
9431
9641
9878
10088
10176
10684
11324
11920
11921
12113
12367
12515
12665
13813
14409





ejercicioRSA5.2.1

Contando solamente con el software Fortaleza de Cifrados, encuentra los 49 números no cifrables de la clave RSA con $p = 409$, $q = 499$, $e = 31$ que has generado en la prácticaRSA5.2.1.

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

$$\sigma_n = [1 + \text{mcd}(e-1, p-1)][1 + \text{mcd}(e-1, q-1)]$$

Los números no cifrables serán:

$$N = [q\{\text{inv}(q, p)\}N_p + p\{\text{inv}(p, q)\}N_q] \bmod n$$

con: N_p las soluciones de $N^e \bmod p = N$

N_q las soluciones de $N^e \bmod q = N$

CLAVE GENERADA

Número primo P generado: 409
Número primo Q generado: 499
Componente (módulo n) generado: 204091
Componente d privado generado: 19663
Componente e generado: 31

MENSAJES NO CIFRABLES

El número de Mensajes no cifrables va a ser: 49

0	49899	96168	121117	155828
1	56388	97804	121118	177505
1636	58024	97805	122753	179141
1637	72855	99440	122754	179142
23313	74491	99441	124390	180777
23314	79701	104650	129600	180778
24949	81337	104651	131236	202454
24950	81338	106286	146067	202455
26586	82973	106287	147703	204090
48263	82974	107923	154192	

LECCIÓN 5. MENSAJES NO CIFRABLES

Apartado 5.3. Minimizando los números no cifrables



prácticaRSA5.3.1

Con el software genRSA comprueba las siguientes claves RSA cuyos valores de p y q son primos seguros, en las que se han usado todos los valores posibles y válidos de la clave pública e.

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

Clave RSA1: p = 5, q = 7	Valores de clave pública: $2 < e < 35$
Clave RSA1: p = 5, q = 11	Valores de clave pública: $2 < e < 55$
Clave RSA1: p = 7, q = 11	Valores de clave pública: $2 < e < 77$
Clave RSA1: p = 5, q = 23	Valores de clave pública: $2 < e < 115$
Clave RSA1: p = 23, q = 59	Valores de clave pública: $2 < e < 1.357$

¿Qué sucede con la cantidad y proporción de valores de la clave pública e que dan como resultado sólo 9 números no cifrables a medida que aumentan de tamaño los valores de p y q?

Ejemplo: Clave RSA1: p = 7, q = 11

$$p = 7 = (2r + 1) = (2 \cdot 3 + 1) \text{ con } r = 3$$

$$q = 11 = (2s + 1) = (2 \cdot 5 + 1) \text{ con } s = 5$$

$$\text{NNC} = (1 + 2)(1 + 2) = 9 \quad e = 17, 23, 29, 47, 53, 59$$

$$\text{NNC} = 3(2 \cdot r + 1) = 3(2 \cdot 3 + 1) = 21 \quad e = 7, 13, 19, 37, 43, 49$$

$$\text{NNC} = 3(2 \cdot s + 1) = 3(2 \cdot 5 + 1) = 33 \quad e = 11, 41$$

$$\text{NNC} = (2 \cdot r + 1)(2 \cdot s + 1) = (2 \cdot 3 + 1)(2 \cdot 5 + 1) = 77 \quad e = 31$$



prácticaRSA5.3.2

Con el software genRSA genera estas claves en las que la clave pública $e = \phi(n)/2 + 1$ y observa que sucede con la cantidad de números no cifrables $\sigma(n)$. En todo caso, comprueba que se da esa relación entre e y $\phi(n)$.

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

Clave de 20 bits: $p = 937$, $q = 991$, $e = 463321$

Clave de 22 bits: $p = 1493$, $q = 1499$, $e = 1117509$

Clave de 24 bits: $p = 3863$, $q = 4007$, $e = 7735587$

Clave de 26 bits: $p = 7499$, $q = 7057$, $e = 26452945$

Clave de 28 bits: $p = 11743$, $q = 14731$, $e = 86479831$

Clave de 30 bits: $p = 26209$, $q = 28447$, $e = 372756385$

Clave de 32 bits: $p = 60343$, $q = 61091$, $e = 1843146391$

Clave de 64 bits: $p = \text{E2BE51B1}$, $q = \text{BAABE269}$, $e = \text{52AB428148FF47C1}$ (hexa)

Observa en este último caso el error que entrega el programa al indicar el Número de Mensajes no Cifrables. ¿Cuál es el valor verdadero?

LECCIÓN 5. MENSAJES NO CIFRABLES

Apartado 5.4. ¿Hay que preocuparse por estos números no cifrables?



prácticaRSA5.4.1

Con el software genRSA genera estas tres claves de tamaños estándar y observa la cantidad de números no cifrables $\sigma(n)$.

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

IMPORTANTE: Comprueba bien los valores de p y q al copiar y pegar. Adobe comete un error y no copia el último número en claves 1 y 2. En el caso de valores de 1.024 bits es peor: no lo hace además con un par de bits centrales. En la clave 3, haz doble clic al comienzo del número p y luego al final del mismo número y observarás ese error. Lo siento, no puedo hacer nada, es un fallo de Adobe Acrobat :-)

Clave 1:

```
1CC0C6A8909BE5B660807C6156F93DDDE67D4F08877AFD4C0752B0C721A31AA951CCB5DEE7AD6CEE5
BAE9721E0022DE63B2D3575D6C37EB410739057D845E24C7C01
06F90C2DB8C3537D9ED1226721C4175DFC37F077FC95FF1211DBD9BEA59F4F572C529F71FDC2EBF960
E2E91AE8CEDD5E030AC416CF0AD2FB2FF81F151FB1E1
10001
```

Clave 2:

```
CB71C1D96D4B530774C47D0155E9EE4ED48514326A38DE6D2FC9C525FEBD0D20D329483677C41D066
04047E9D2DBE0244B31E0621E54E1615E1E25EBFDC6D961
DCB620812EA9E4A0D4F48B4D214B0C78DCA78D7C81E978E9EFC0D08661CCC6969F04875B765559D96
58BE6DC9975D73C1C44A5604935AC0183708230262F8741
10001
```

Clave 3:

```
BF11FD9D42B665A1C2D37194E99F8EFBBA5C04D0D47F86CAA41107DFDA55D00819ABD044F3B433DF1
4B736F4BD443931751715DAFB3EB1107E7FD05410F42D4759F8CAB3884785CF8F60ECBF902E525B92E8
2331793674CD3595DE3839FC8DBE2FC094F4EAB583FA9C963CFE49A602017B98D3DE38ACF888311CDA
933CB61801
D44899272991BEF647DA3AC06F10D57FC68E0813B8E7B52D48DF166DA4BAF4C7FDBA192B95E307651
A01EA4232ECCCF4570B08B7E51701B5712113275DD7CABEA90352410C542F7744612E47AAEB9C1E096
2B591B0AB5F44C621190ADED2E4DCB2B2EB1B66E9EF46E02EF19FE94ADC5859DF9E9422C39A1EFE60
E5C504B89D9
10001
```