CRYPT4YOU

DOCUMENTO ANEXO A LA LECCIÓN 3

DEL CURSO "EL ALGORITMO RSA"

EJERCICIOS Y PRÁCTICAS PROPUESTOS Y RESUELTOS

Autor: Dr. Jorge Ramió Aguirre
Fecha de publicación: 12 de abril de 2012
http://www.criptored.upm.es/crypt4you/temas/RSA/leccion3/leccion03.html

TABLA DE CONTENIDOS

Creative Commons (*CC*) - *NoCommercial-Attribution-ShareAlike*

LECCIÓN 3. CIFRADO DE NÚMEROS Y MENSAJES

Apartado 3.1. El intercambio de clave de Diffie y Hellman

prácticaRSA3.1.1

Descarga e instala el software ExpoCrip en la carpeta Criptolab, es decir, C:\Criptolab\ExpoCrip.
SW ExpoCrip: http://www.criptored.upm.es/software/sw_m001l.htm
Importante: Si estás trabajando con Windows 7 y 64 bits, es posible que recibas mensajes de error por la falta de los archivos comdlg32.ocx y tabctl32.ocx. Si es así, por favor instala versiones recientes de estos ocx. En esta página encontrarás el archivo comdlg32.ocx y las indicaciones de cómo hacerlo:
http://devonenote.com/2010/02/register-comdlg32-ocx-on-x64-win7/
Y en esta otra página el archivo tabctl32.ocx:
http://www.ocxdump.com/download-ocx-files_new.php/ocxfiles/T/TABCTL32.OCX/6.01.9782/download.html
Para el registro de cada programa, debes tener permiso de administrador: debes ejecutar como administrador desde el botón derecho en el icono del sistema de tu PC.

Pincha en las herramientas del software ExpoCrip y comprueba que los siguientes 4 números son primos; a continuación encuentra sus raíces primitivas.

13; 181; 7.001; 12.037

Repite estos cálculos para estos primos seguros:

83; 863; 4.127; 12.263

¿Cuántas raíces has encontrado en cada caso? ¿Ves alguna diferencia al trabajar con primos seguros?

Creative Commons (*CC*) - *NoCommercial-Attribution-ShareAlike*

ejercicioRSA3.1.1

Con la calculadora de Windows simula el siguiente intercambio de clave.

1. Alicia y Bernardo eligen el primo 7.001 y un generador α = 101.
2. Alicia elige el valor a = 49.
3. Bernardo elige el valor b = 77.
4. ¿Qué clave secreta se intercambian al terminar el protocolo?

   Valores intermedios: 1.358, 2.434, 5.243, 5.243.

Usando ahora el software Fortaleza de Cifrados simula el siguiente intercambio de clave.
No se incluyen los puntos para que puedas copiar y pegar:
SW Fortaleza de Cifrados: http://www.criptored.upm.es/software/sw_m001e.htm

1. Alicia y Bernardo eligen el primo 9998931707 y un generador α = 20.
2. Alicia elige el valor a = 1234.
3. Bernardo elige el valor b = 4321.
4. ¿Qué clave secreta se intercambian al terminar el protocolo?

   Valores intermedios: 3.429.729.571, 7.495.753.609, 4.557.790.162, 4.557.790.162.

Usando el software Fortaleza de Cifrados simula este otro intercambio de clave.

1. Alicia y Bernardo eligen el primo 810346749275979232714980036156441026521 9 de 40 dígitos y un generador α = 22.
2. Alicia elige el valor a de 25 dígitos = 9872765378564442787382019.
3. Bernardo elige el valor b de 25 dígitos = 5344628353427342804508240.
4. ¿Qué clave secreta se intercambian al terminar el protocolo?
5. ¿De cuántos bits sería esta clave que se intercambian Alicia y Bernardo?

   Valores intermedios:
   1149271436090773793823222550696842308582
   8500884282608156223892326605111732054 49
   7742867783938989693252454245257811576523
   7742867783938989693252454245257811576523

Creative Commons (*CC*) - *NoCommercial-Attribution-ShareAlike*

ejercicioRSA3.1.2

Usando la calculadora de Windows Alicia enviará la clave 15 a Bernardo usando el protocolo de Diffie y Hellman modificado.

Alicia: $p_A = 113$; $\alpha_A = 10$; $a = 35$
Calcula la clave pública de Alicia: $\alpha_A^{\ a} \bmod p_A =$ _____
Bernardo: $p_B = 211$; $\alpha_B = 7$; $b = 29$
Calcula su clave pública de Berbardo: $\alpha_B^{\ b} \bmod p_B =$ _____
Paso 1. $K_{AB} = (\alpha_B^{\ b} \bmod p_B)^a \bmod p_B = \alpha_B^{\ ba} \bmod p_B =$ _____
Paso 2. Alicia envía a Bernardo: $\alpha_B^{\ a} \bmod p_B =$ _____
Paso 3. Bernardo calcula $(\alpha_B^{\ a} \bmod p_B)^b \bmod p_B =$ _____
Clave intercambiada $K_{AB} =$ _____

Repite el ejercicio usando ahora el software Fortaleza de Cifrados. No se incluyen los puntos para que puedas copiar y pegar. ¿qué clave se intercambia ahora?
SW Fortaleza de Cifrados: http://www.criptored.upm.es/software/sw_m001e.htm

Alicia: $p_A = 14808607715315782481$; $\alpha_A = 33$; $a = 825400834721$
Calcula la clave pública de Alicia: $\alpha_A^{\ a} \bmod p_A =$ _____
Bernardo: $p_B = 26831423036065352611$; $\alpha_B = 42$; $b = 837209217633$
Calcula su clave pública de Berbardo: $\alpha_B^{\ b} \bmod p_B =$ _____
Paso 1. $K_{AB} = (\alpha_B^{\ b} \bmod p_B)^a \bmod p_B = \alpha_B^{\ ba} \bmod p_B =$ _____
Paso 2. Alicia envía a Bernardo: $\alpha_B^{\ a} \bmod p_B =$ _____
Paso 3. Bernardo calcula $(\alpha_B^{\ a} \bmod p_B)^b \bmod p_B =$ _____
Clave intercambiada $K_{AB} =$ _____

Creative Commons (*CC*) - *NoCommercial-Attribution-ShareAlike*

LECCIÓN 3. CIFRADO DE NÚMEROS Y MENSAJES

Apartado 3.2. Implementación del intercambio de clave con RSA

prácticaRSA3.2.1

Simula el envío de una clave de sesión de 128 bits a un servidor que nos muestra una clave RSA de 1.024 bits usando el software genRSA.
SW genRSA: http://www.criptored.upm.es/software/sw_m001d.htm

Datos de la clave del servidor:
p =
E9C898ECD1F3CD6C39466EF78BB72EC829EBA5668E4444C8E11B8EBDC94A858B84EE63D633
6B8BC478B0BF5F43BC933BE96022587747FF4945356F96CE8CD58F.
q =
F5C466DD1199CB464DBE0CB6AAE42504323A9E6EBA8E17DD17B5256B8F2E5C228E02AD069
AEEF35689C4C810F20F9DB3E1F60A48CF6362A3D1648BE70FD10C7F.
e = 010001.
Clave de sesión a intercambiar: K = 12345678900000000000000000000987654321.

IMPORTANTE: comprueba y revisa los valores p y q que copias en la aplicación y añade el valor que falta. Como ya vimos en una lección anterior, Adobe Acrobat tiene un bug al seleccionar un número grande y copiarlo al portapapeles dejando fuera el último elemento hexadecimal, algo que no sucede con el archivo Word.

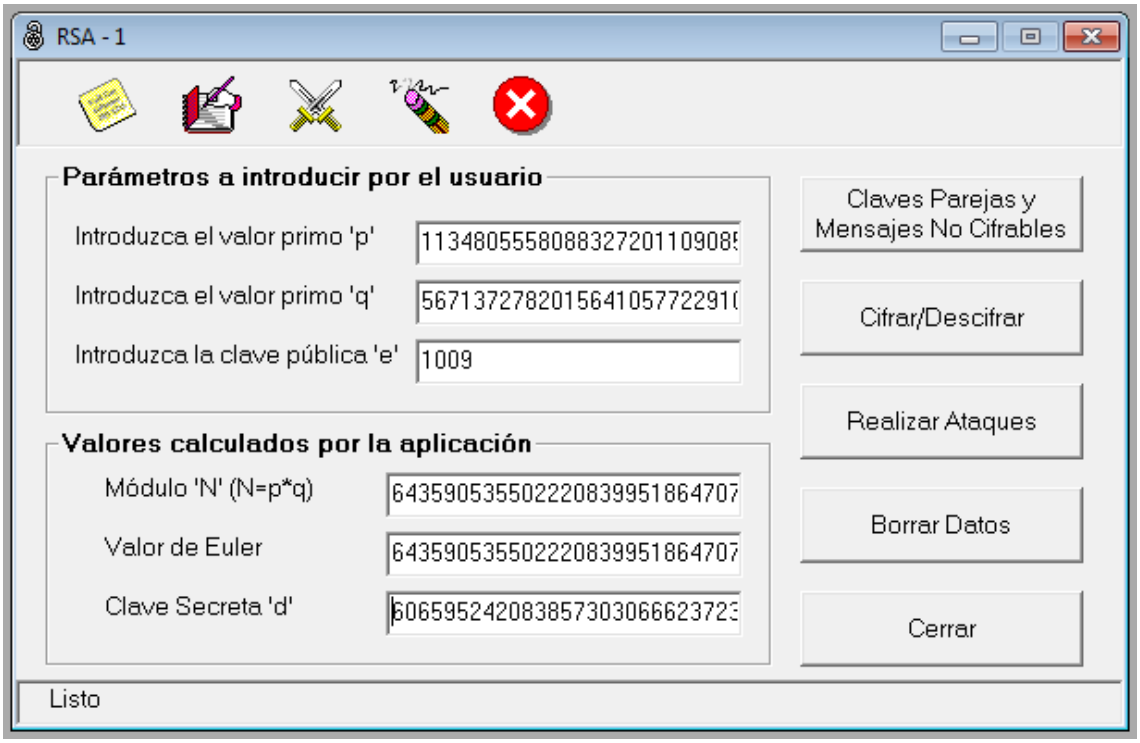
Creative Commons (*CC*) - *NoCommercial-Attribution-ShareAlike*

prácticaRSA3.2.2

Vas a repetir el envío de la clave de la práctica3.2.1 usando ahora el software ExpoCrip con una clave RSA un poco más pequeña.
SW ExpoCrip: http://www.criptored.upm.es/software/sw_m001l.htm

Datos de la clave del servidor:
p = 1134805558088327201109085605317536111 3.
q = 567137278201564105772291012386280352 43.
e = 1009.
Clave de sesión a intercambiar: K = 123456789000000000000000000000987654321.

1. En ExpoCrip pinchamos en el primer icono en la parte superior, candado Criptosistema RSA.
2. Introducimos los valores de p y de q. Pulsamos TAB y nos muestra el módulo.
3. Introducimos la clave pública e. Pulsamos TAB y nos muestra la clave privada.
4. Activamos opción Cifrar/Descifrar y elegimos Cifrar Números. Introducimos K y cifra mos.
5. Copiamos el criptograma C, lo pegamos como entrada y elegimos luego descifrar.



Creative Commons (*CC*) - *NoCommercial-Attribution-ShareAlike*

prácticaRSA3.2.3

Usa ExpoCrip para enviar cifrada una clave de sesión K de 192 bits (58 dígitos) a un servidor Web cuya clave es el último desafío RSA resuelto de 768 bits en diciembre de 2001, y cuyos números primos se indican. Web: http://www.rsa.com/rsalabs/node.asp?id=3723

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

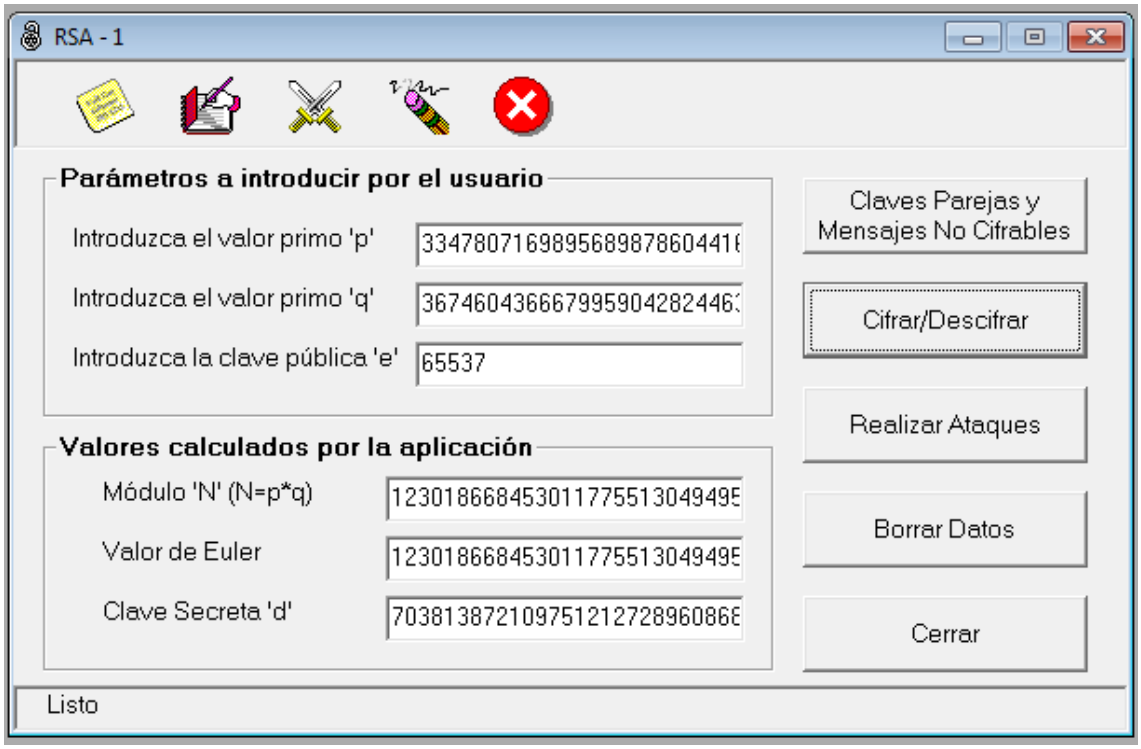
p = 33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489.

q = 36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917.

Nota: A diferencia de genRSA este programa tarda bastante en confirmar que p y q son primos.

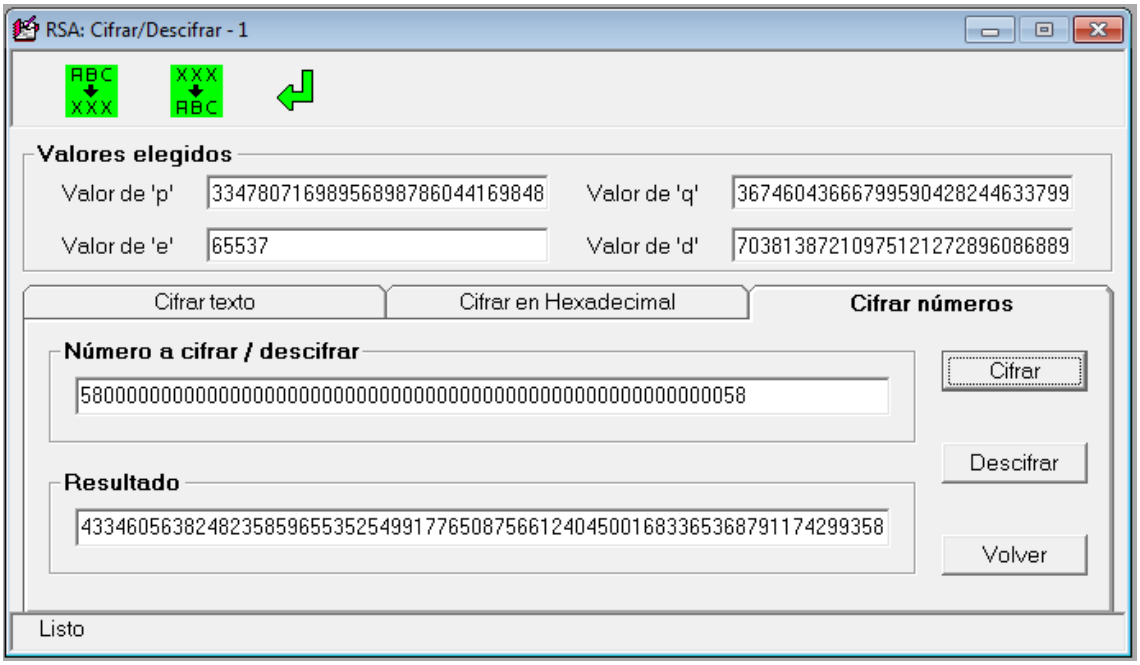
e = 65537.

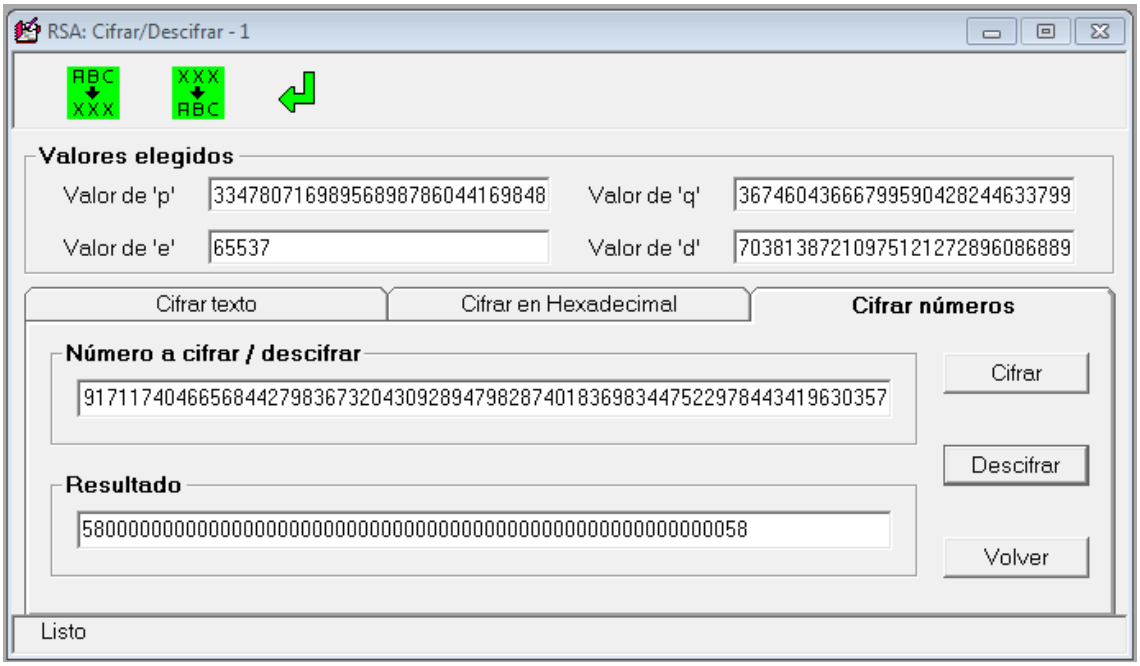
K = 5800000000000000000000000000000000000000000000000000000000000058.



Creative Commons (CC) - NoCommercial-Attribution-ShareAlike

1. Cifra la clave K con la clave pública del servidor.
2. Recupera luego la clave K.
   Observación: el programa ExpoCrip tardará algunos segundos en entregar la solución.
   Recuerda que se trata sólo de una aplicación de laboratorio y educativa, no comercial.
3. ¿Por qué crees que tarda mucho más en descifrar que en cifrar?
4. ¿Por qué crees que tarda más que genRSA en comprobar que p y q son primos?





LECCIÓN 3. CIFRADO DE NÚMEROS Y MENSAJES

Apartado 3.3. Cifrando mensajes con RSA

ejercicioRSA3.3.1

Encuentra los tamaños de bloques de cifra de mensajes con RSA, dependiendo de que el bloque se forme con un número entero de bytes o bien se cifre en un cuerpo un dígito menor que el módulo

Caso 1: cifra con bloques de bytes completos

- RSA1: p = 2297, q = 7109
- RSA2: p = 101653; q = 1238761
- RSA3: p = 121793911; q = 4538991421

Caso 1: cifra con bloques de tamaño un dígito menor que el módulo

- RSA1: p = 21169, q = 87421
- RSA2: p = 1101811; q = 4744297
- RSA3: p = 3770202641; q = 6156182033

Creative Commons (*CC*) - *NoCommercial-Attribution-ShareAlike*

prácticaRSA3.3.1

Con el software genRSA y luego con ExpoCrip cifra y descifra el mensaje de texto de 18 caracteres CALCULANDO BLOQUES. Observa cómo se forman los bloques en ExpoCrip.

SW genRSA: http://www.criptored.upm.es/software/sw_m001d.htm
SW Fortaleza de Cifrados: http://www.criptored.upm.es/software/sw_m001e.htm
SW ExpoCrip: http://www.criptored.upm.es/software/sw_m001l.htm
SW Online conversion utilities: http://www.darkfader.net/toolbox/convert/
SW Conversor dec2hex: http://www.criptored.upm.es/software/sw_m051b.htm

Con software genRSA:

1. Genera esta clave RSA: p = 5923; q = 6689; e = 31.
2. Cifra el mensaje M = CALCULANDO BLOQUES.
   Preguntas:
3. ¿De qué tamaño ha sido el bloque a cifrar?
4. Con el software Fortaleza de Cifrados comprueba el cifrado y descifrado de los dos primeros bloques.
5. Comprueba qué sucede si en el texto en claro incluimos el punto final.

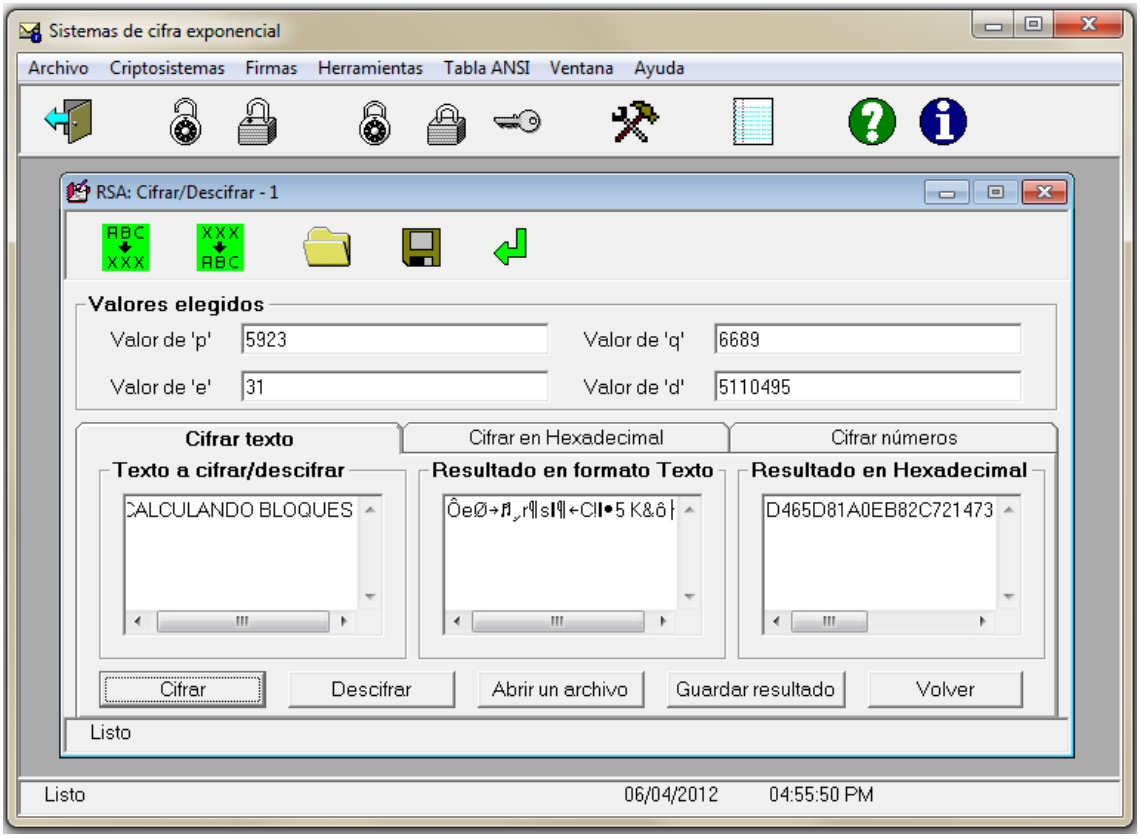
Con software ExpoCrip:

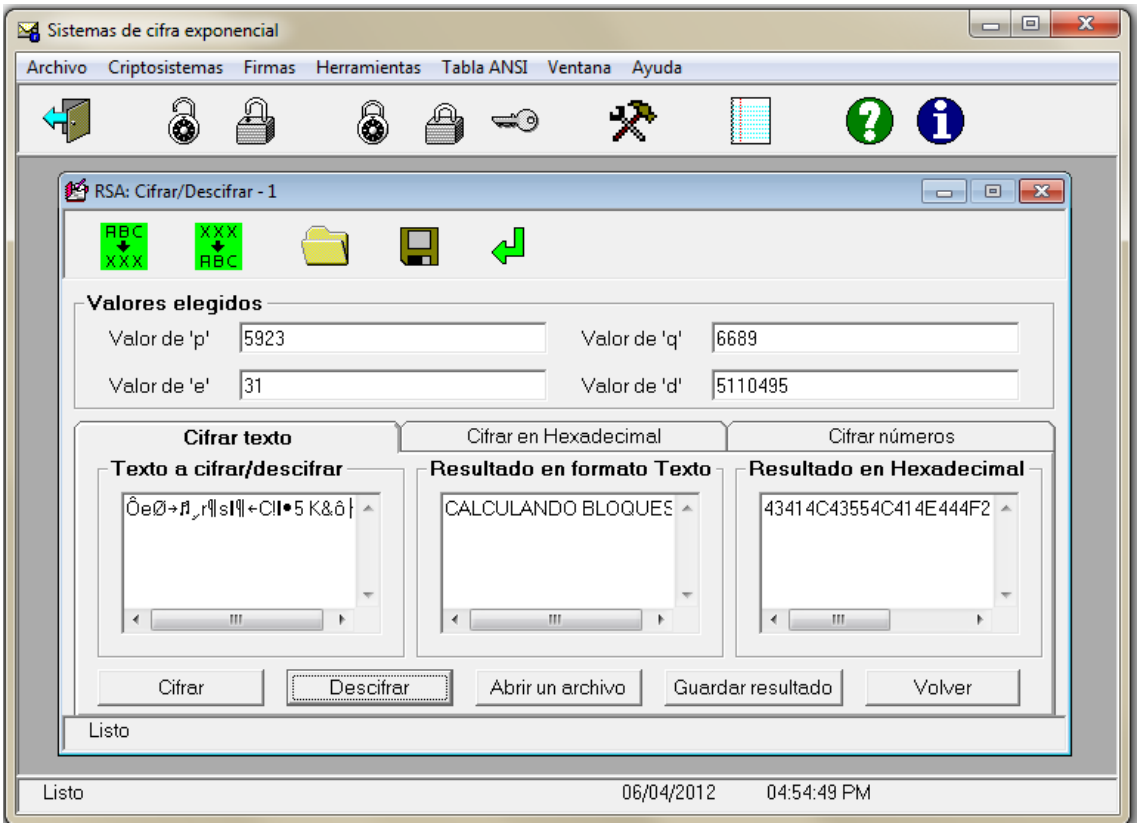
1. Genera la clave RSA: p = 5923; q = 6689; e = 31.
2. Cifra el mensaje M = CALCULANDO BLOQUES.

Pasos:

1. En el primer icono del candado abierto de ExpoCrip introducimos los valores de p, q y e pulsando en cada ocasión la tecla TAB, generándose así la clave.
2. En la opción Cifrar/Descifrar elegimos Cifrar texto e introducimos el mensaje CALCULANDO BLOQUES.
3. Al pulsar el botón Cifrar se obtiene el siguiente criptograma en hexadecimal.
   C = D465D81A0EB82C72147395141B43218A0735A04B26F419.
   Y el resultado en formato texto donde están representados todos los caracteres ASCII, incluido el salto de línea aquí quitado: C = ÔeØ¸,rs•C!Š5 K&ô.
4. Para descifrar, copiamos al portapapeles el criptograma que nos muestra en formato texto y lo pegamos como entrada de Texto a Cifrar/Descifrar.
5. Pulsamos el botón Descifrar para recuperar el texto en claro.

Creative Commons (*CC*) - *NoCommercial-Attribution-ShareAlike*


Sistemas de cifra exponencial
Archivo Criptosistemas Firmas Herramientas Tabla ANSI Ventana Ayuda
RSA: Cifrar/Descifrar - 1
Valores elegidos
Valor de 'p' 5923
Valor de 'q' 6689
Valor de 'e' 31
Valor de 'd' 5110495
Cifrar texto
Cifrar en Hexadecimal
Cifrar números
Texto a cifrar/descifrar
Resultado en formato Texto
Resultado en Hexadecimal
CALCULANDO BLOQUES
D465D81A0EB82C721473
Cifrar
Descifrar
Abrir un archivo
Guardar resultado
Volver
Listo
Listo 06/04/2012 04:55:50 PM


Sistemas de cifra exponencial
Archivo Criptosistemas Firmas Herramientas Tabla ANSI Ventana Ayuda
RSA: Cifrar/Descifrar - 1
Valores elegidos
Valor de 'p' 5923
Valor de 'q' 6689
Valor de 'e' 31
Valor de 'd' 5110495
Cifrar texto
Cifrar en Hexadecimal
Cifrar números
Texto a cifrar/descifrar
Resultado en formato Texto
Resultado en Hexadecimal
CALCULANDO BLOQUES
43414C43554C414E444F2
Cifrar
Descifrar
Abrir un archivo
Guardar resultado
Volver
Listo
Listo 06/04/2012 04:54:49 PM

¿Cómo se obtienen los bloques de cifrado en ExpoCrip?

Con el software Online conversion utilities obtenemos que:
M = CALCULANDO BLOQUES = 43414C43554C414E444F20424C4F51554553 (hexadecimal)

Con el software dec2hex pasamos este número hexadecimal a decimal:

C:\Program Files\Java\jre6\bin>java -jar c:/Criptolab/dec2hex/dec2hex.jar -h
43414C43554C414E444F20424C4F51554553

= 585874288221941306869462134821697725433582 7 (Mensaje M en decimal)

Como n = 39.618.947, haremos bloques de 7 dígitos partiendo desde el final hacia el comienzo:

5 8587428 8221941 3068694 6213482 1697725 4335827 (Mensaje M en decimal)

Con el software Fortaleza de Cifrados ciframos los siete bloques. Como estamos en un módulo de 8 dígitos, todos los resultados de la cifra se indicarán con 8 dígitos. Así, si algún resultado tiene menos de 8 dígitos, se le añaden tantos ceros a la izquierda como sea necesario.

5^{31} mod 31 mod 39.618.947 = 20.343.670
$8.587.428^{31}$ mod 31 mod 39.618.947 = 33.592.353
$8.221.941^{31}$ mod 31 mod 39.618.947 = 29.330.045
$3.068.694^{31}$ mod 31 mod 39.618.947 = 31.086.393
$6.213.482^{31}$ mod 31 mod 39.618.947 = 18.652.028
$1.697.725^{31}$ mod 31 mod 39.618.947 = 15.775.907
$4.335.827^{31}$ mod 31 mod 39.618.947 = 6.598.937 (aquí deberá agregarse 1 relleno: **0**6.598.937)

Por tanto, el número entero será la concatenación de los siete bloques cifrados, es decir:
2034367033592353293300453108639318652028157759070 6598937

Con el software dec2hex pasamos ese valor a hexadecimal:

C:\Program Files\Java\jre6\bin>java -jar c:/Criptolab/dec2hex/dec2hex.jar
20343670335923532933004531086393186520281577590706598937

= D465D81A0EB82C72147395141B43218A0735A04B26F419

Que es el criptograma C que se observa en ExpoCrip representado en hexadecimal.

Creative Commons (*CC*) - *NoCommercial-Attribution-ShareAlike*