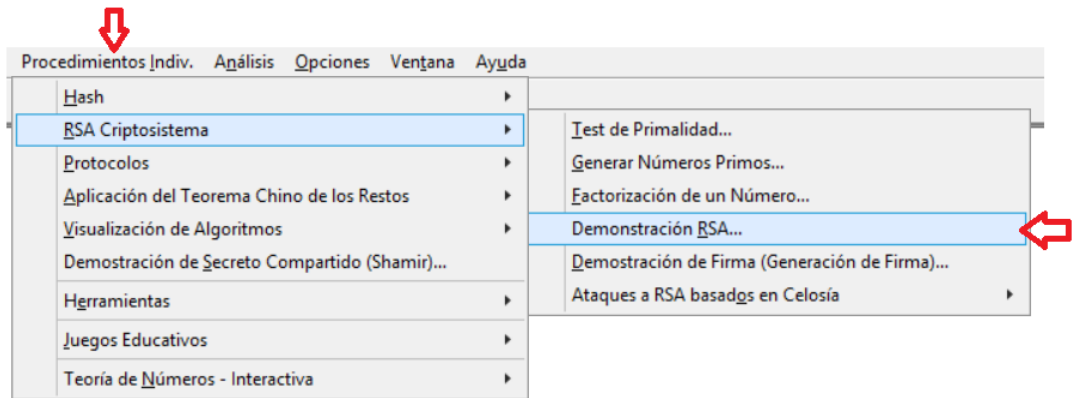
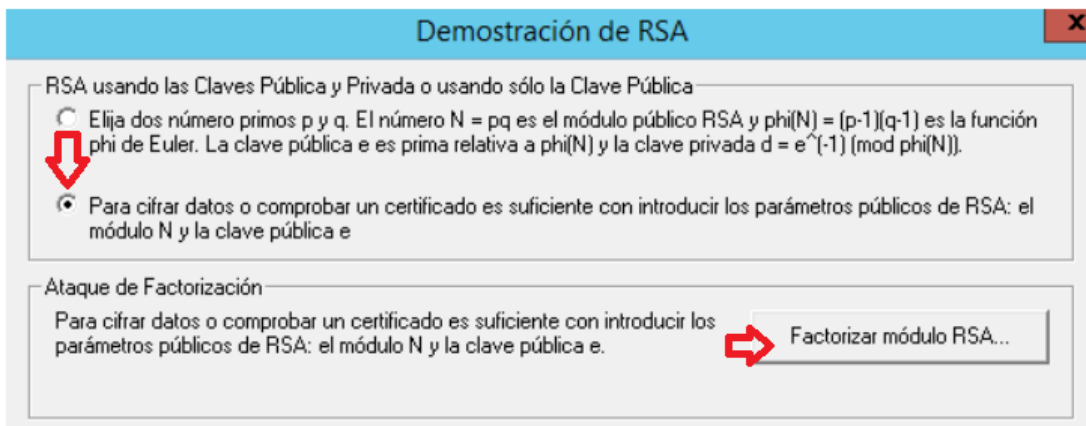



```
Raw text
N=3404062474937242861395243981141418377549190749193
e = 2^16 + 1
0699647424488547213538018687288179468997406246529 #
1602895004162842681114653387147102789102453404163 #
2094836235654395727458589429933425704847883731085 #
1750607186559703713851933077207983420223532519062
```

Por ello, a continuación utilizamos una herramienta como Cryptool. Tenemos que pulsar en la pestaña “Procedimientos Indiv.”, luego en “RSA Criptosistema” y finalmente en “Demostración RSA”.



Lo primero que tenemos que hacer ahora es factorizar el módulo RSA mediante la N que conseguimos antes.



Para ello, introducimos este valor y seleccionamos todos los algoritmos de factorización. Después le damos a continuar y en cuestión de segundos habrá terminado,

Factorización de un Número

Algoritmos de Factorización

- Fuerza Bruta
- Algoritmo Brent
- Método Pollard
- Método Williams
- Algoritmo Lenstra
- Método Criba Cuadrática

Entrada

Introduzca el número a factorizar:

Factorización (paso a paso)

Pulsando en el botón 'Continuar' irá viendo qué algoritmos se utilizan para factorizar, en primer lugar el valor de la entrada y después los números en rojo del campo resultado.

Ahora podemos ver que se han generado los números primos p y q , la clave privada y demás parámetros. También tenemos que introducir en el campo de clave pública el valor e que nos aparecía en el decode del QR.

Entrada de número primo

Número primo p	<input style="width: 95%;" type="text" value="1470141949943601597084337"/>	
Número primo q	<input style="width: 95%;" type="text" value="2315465166522070469993689"/>	<input type="button" value="Generar números primos..."/>

Parámetros RSA

RSA módulo N	<input style="width: 95%;" type="text" value="340406247493724286139524398114141837754"/>	(público)
$\phi(N) = (p-1)(q-1)$	<input style="width: 95%;" type="text" value="340406247493724286139524019553430191187"/>	(secreto)
Clave Pública e	<input style="width: 95%;" type="text" value="2^16+1"/>	
Clave Privada d	<input style="width: 95%;" type="text" value="333066973073036240969388867812749402318"/>	<input type="button" value="Actualizar Parámetros"/>

Una vez hecho esto, introducimos las cadenas de números seguidas de las almohadillas y seleccionamos que la entrada es de números. Finalmente le damos a descifrar y nos sale el texto en claro, que contiene la flag que buscábamos.

Cifrado RSA utilizando e / descifrado utilizando d (longitud de alfabeto: 256)

Entrada texto números

Texto cifrado codificado en número de base 10

Descifrar mensaje $m[i] = c[i]^d \pmod N$

El texto de salida del proceso de descifrado (en segmentos de tamaño 20; el símbolo '#' es el usado como separ.

Texto claro



En caso de que no haya salido, pulsamos en Opciones del alfabeto y sistema numérico y nos aseguramos de que las opciones coinciden con las siguientes:

Opciones del Alfabeto

Todos los caracteres ASCII(256) Número de caracteres: 256

Alfabeto específico:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Variante RSA

Normal Diálogo de las Hermanas

Método para codificar un bloque en números

b-ádjco Sistema Numérico

Longitud de bloque

El número de caracteres que es cifrado en cada operación del RSA.
El tamaño máximo está sujeto a la longitud del RSA modulo N en bits, el número de caracteres del alfabeto y el método de codificación empleado.

Longitud de bloque en (Longitud máxima del bloque: 20 caracteres) caracteres:

Sistema Numérico

Los números para las operaciones de cifrado y descifrado RSA serán representados en el siguiente sistema:

Decimal Binario Octal Hexadecimal