CTF HACKON 2021

CRYPTO – ONK ONK ONK

HackOn 2021

https://www.hackon.es/
@HackOnURJC

ENUNCIADO

Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk Onk

FLAG

HackOn{G00se_Game}

SOLUCIÓN

Lo que nos encontramos al descargar el archivo, es un código QR un poco peculiar, pues nuestro móvil no es capaz de detectarlo. Por ello recurrimos a herramientas online que nos ayuden a ello, como https://zxing.org/w/decode.jspx

Subimos la imagen a la página y en seguida nos muestra el contenido decodificado, el cual tiene un dibujo de una oca e información valiosa. Nos encontramos con una *N*, una *e* y cadenas de números, acompañados por almohadillas. Con todo esto podemos deducir de que se trata de un cifrado RSA.

Raw text

N=340406247493724286139524398114141837754919074919 3

e = 2^16 + 1

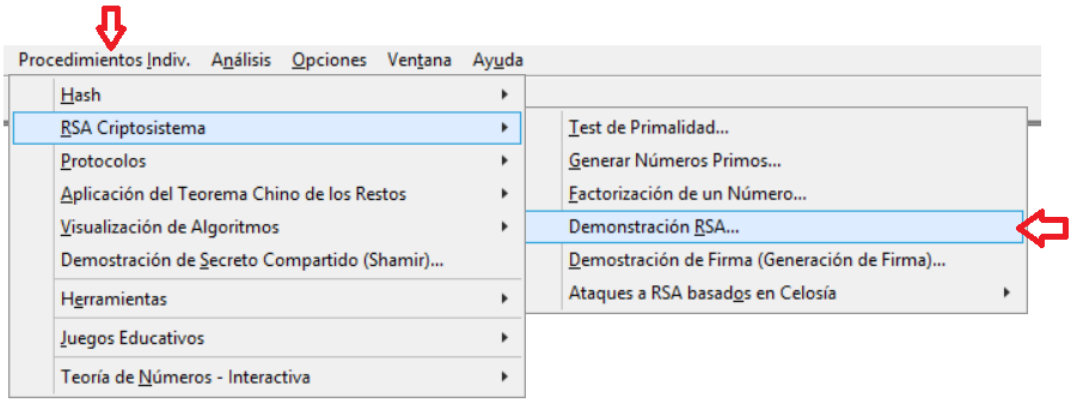
0699647424488547213538018687288179468997406246529 #

160289500416284268111465338714710278910245340416 3 #

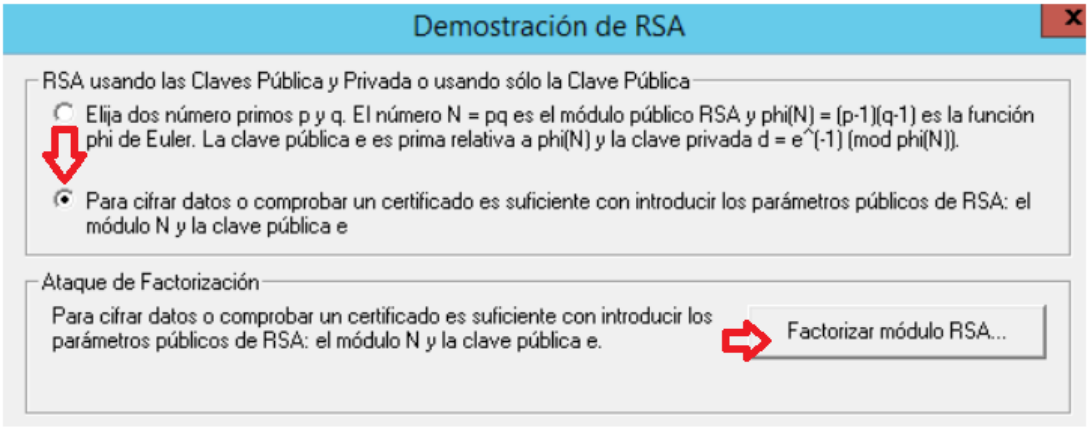
209483623565439572745858942993342570484788373108 5 #

175060718655970371385193307720798342022353251906 2

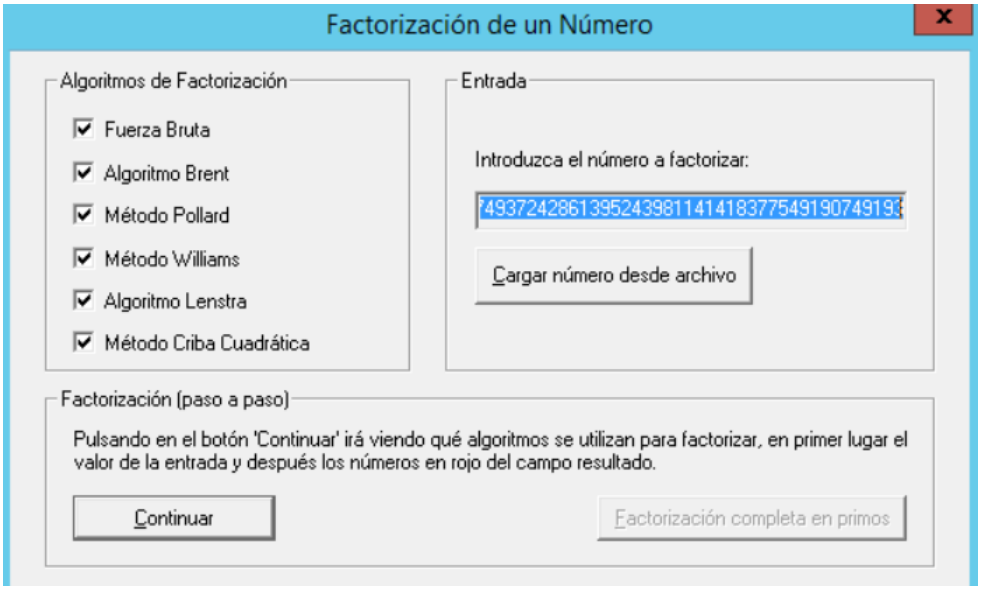
Por ello, a continuación utilizamos una herramienta como CrypTool. Tenemos que pulsar en la pestaña “Procedimientos Indiv.”, luego en “RSA Criptosistema” y finalmente en “Demostración RSA”.



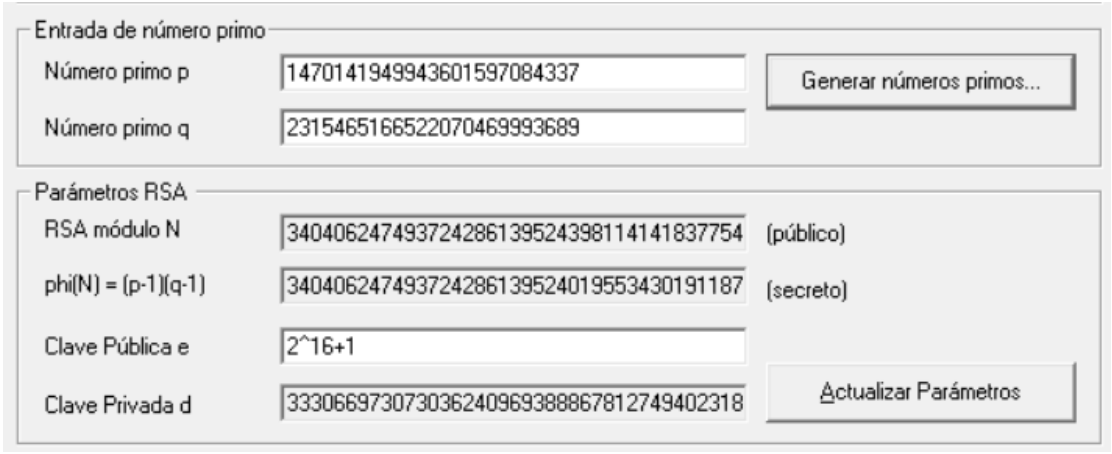
Lo primero que tenemos que hacer ahora es factorizar el módulo RSA mediante la N que conseguimos antes.



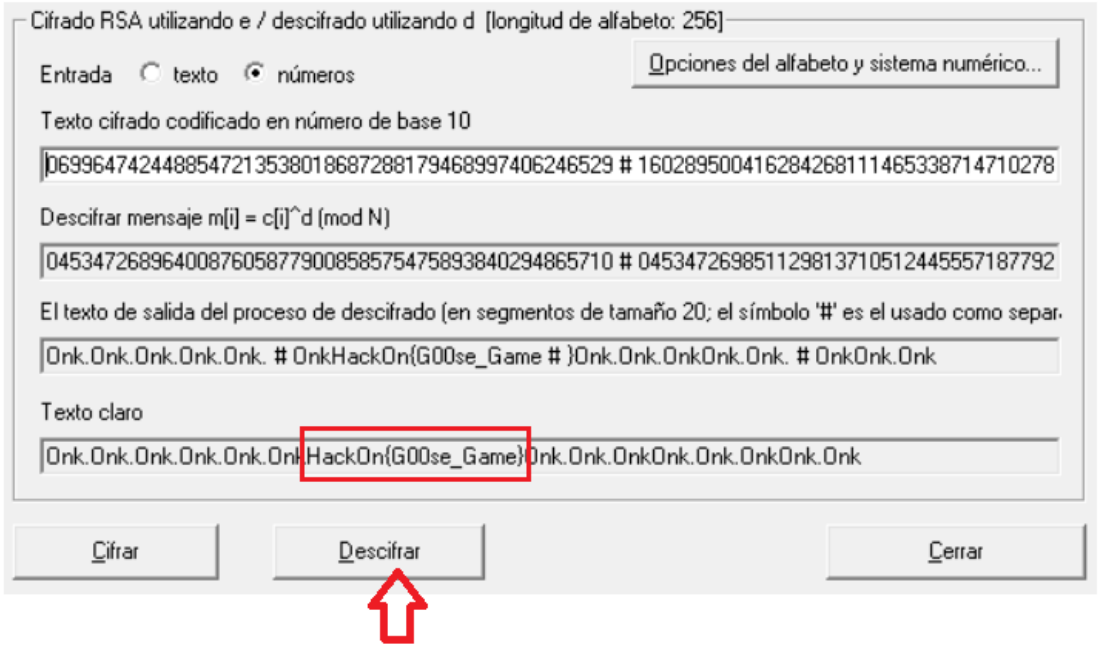
Para ello, introducimos este valor y seleccionamos todos los algoritmos de factorización. Después le damos a continuar y en cuestión de segundos habrá terminado,



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.



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.



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: