Grado en Ingeniería Informática

Seguridad en Tecnologías de la Información
Curso 2017/18

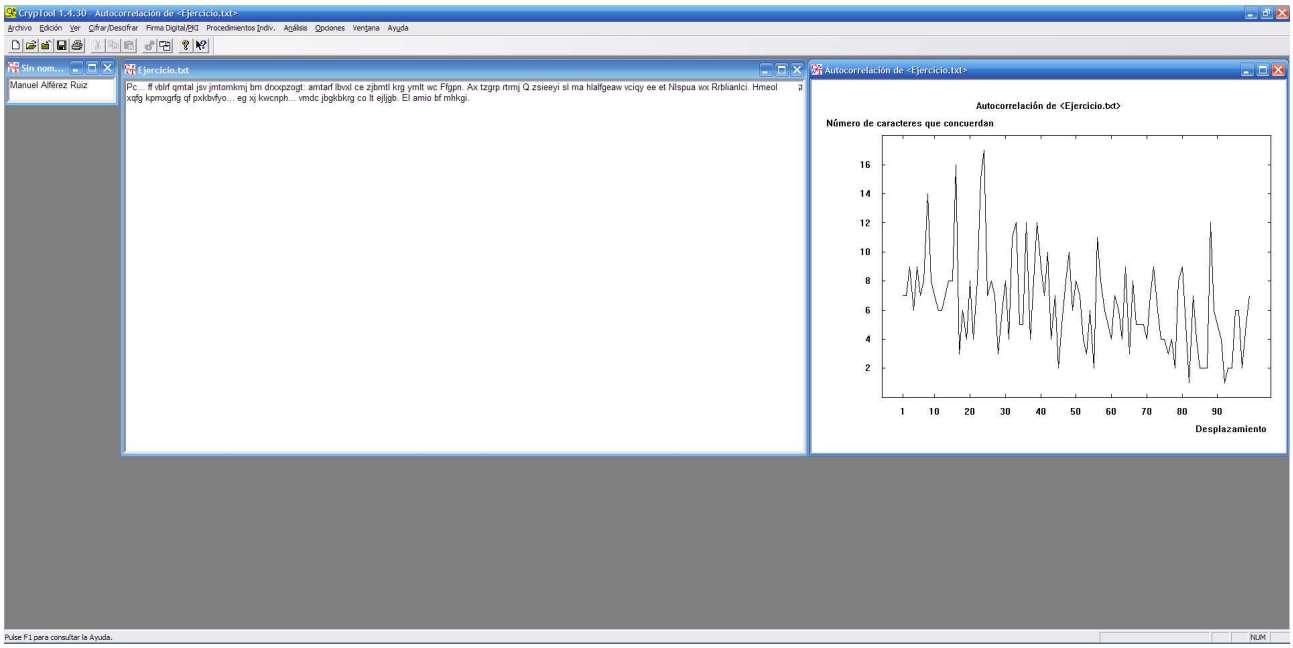
Práctica Número 3

UNIVERSIDAD DE JAÉN

Autor: Manuel Alférez Ruiz

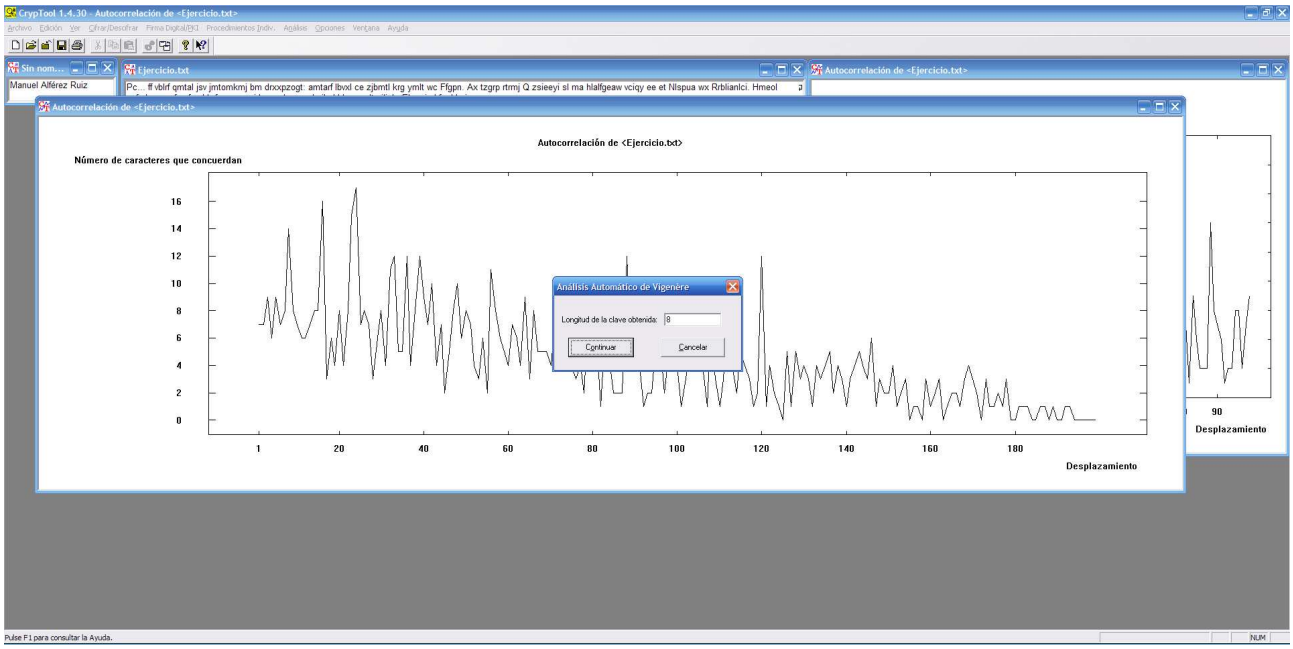
Cifrado polialfabético

En primer lugar cargamos el Ejercicio.txt para realizar el criptoanálisis del mismo, y a continuación *descifrarlo* con el método de *Vigenère*:



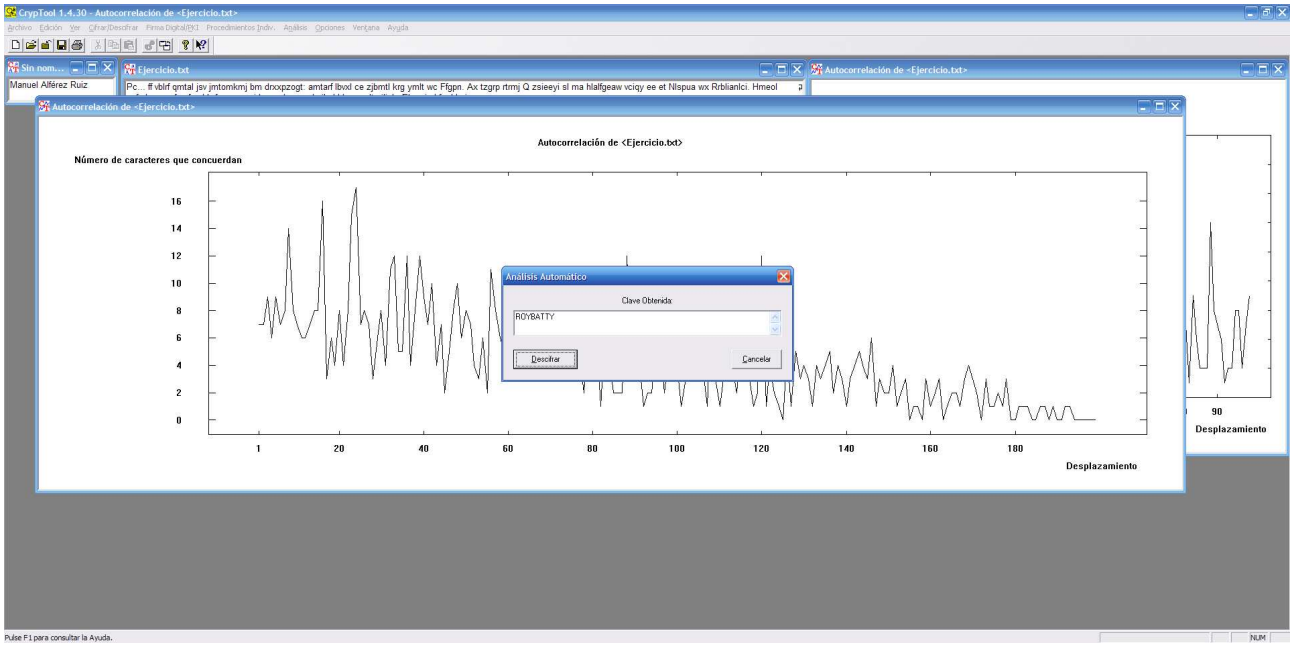
[1.png]

En la imagen podemos ver la gráfica de *autocorrelación*. Procedemos a descifrar el mensaje del archivo Ejercicio.txt:



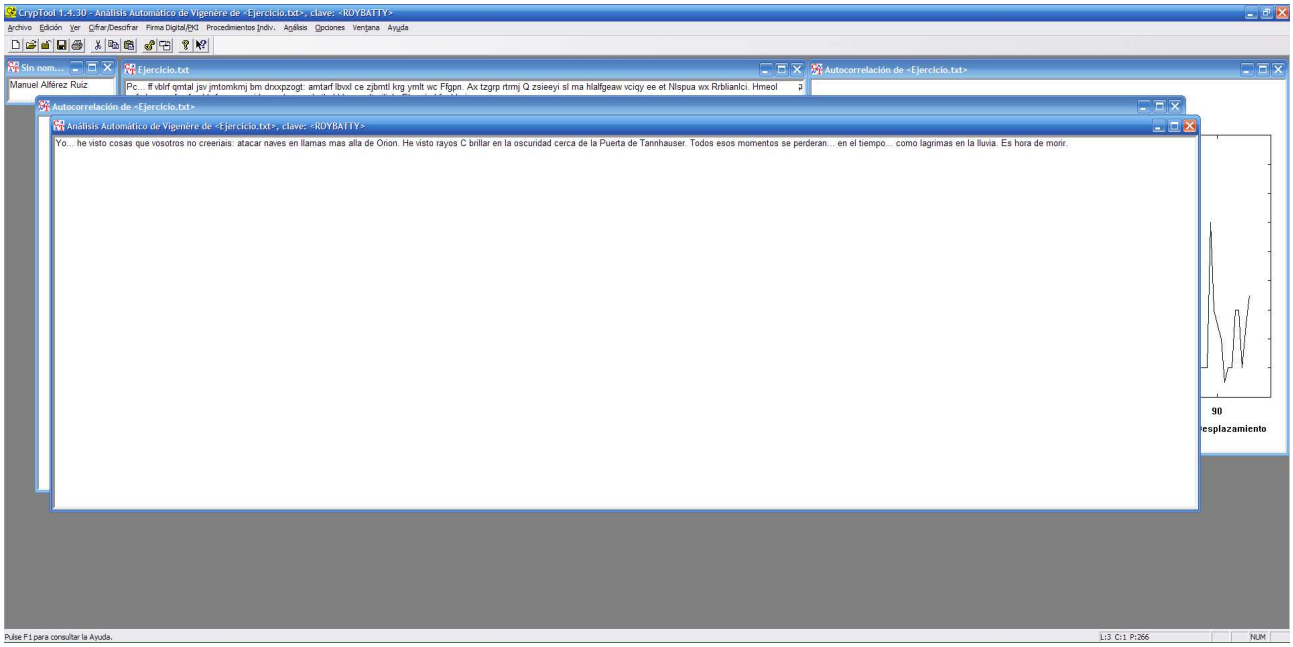
[2.png]

El análisis automático nos calcula una longitud de clave (8). La clave calculada sería:



[3.png]

ROYBATTY, es la clave que descifra el mensaje:

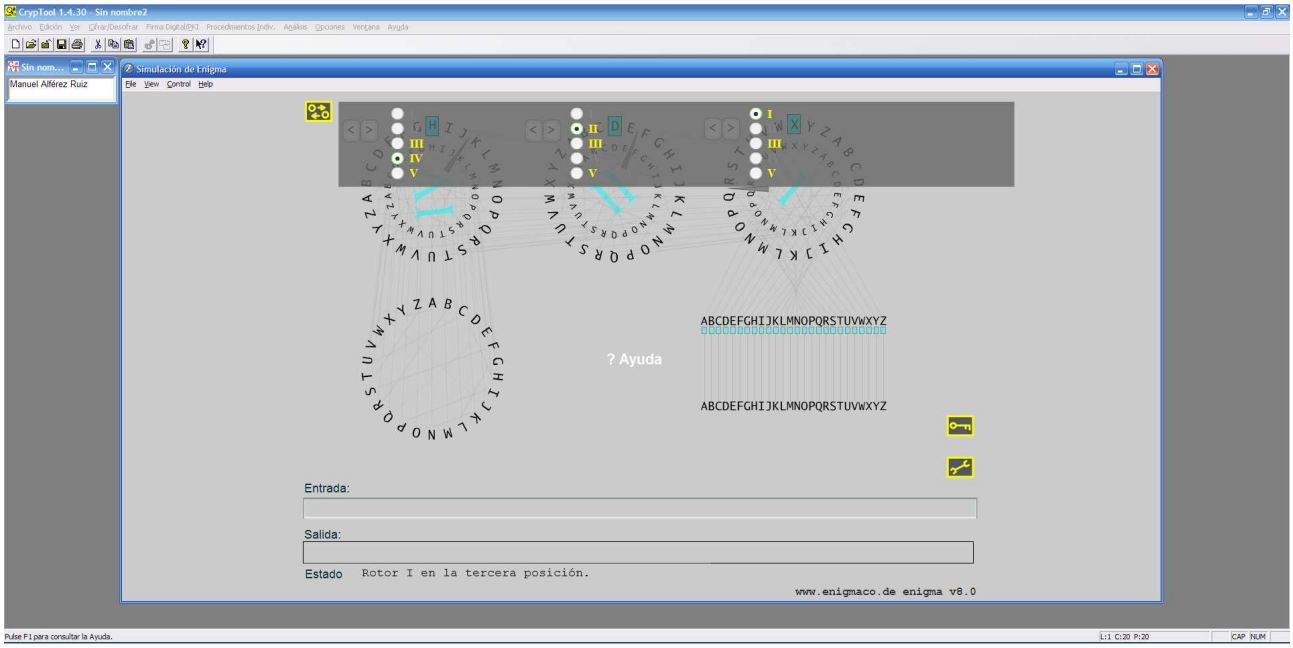


[4.png]

Ya podemos leer el contenido del archivo Ejercicio.txt.

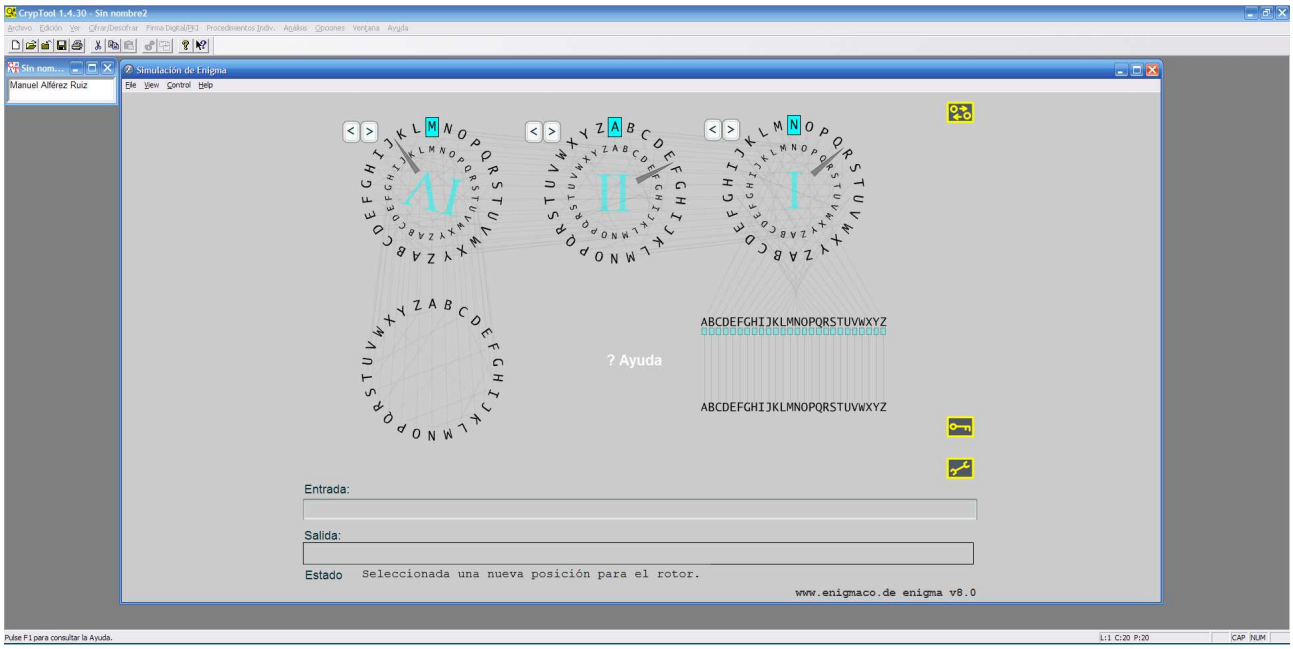
La máquina enigma

En esta segunda parte, procedemos a cifrar un mensaje usando la máquina enigma. Lo primero que debemos de hacer es *ajustar los rotores* con las indicaciones que se nos asignaron:



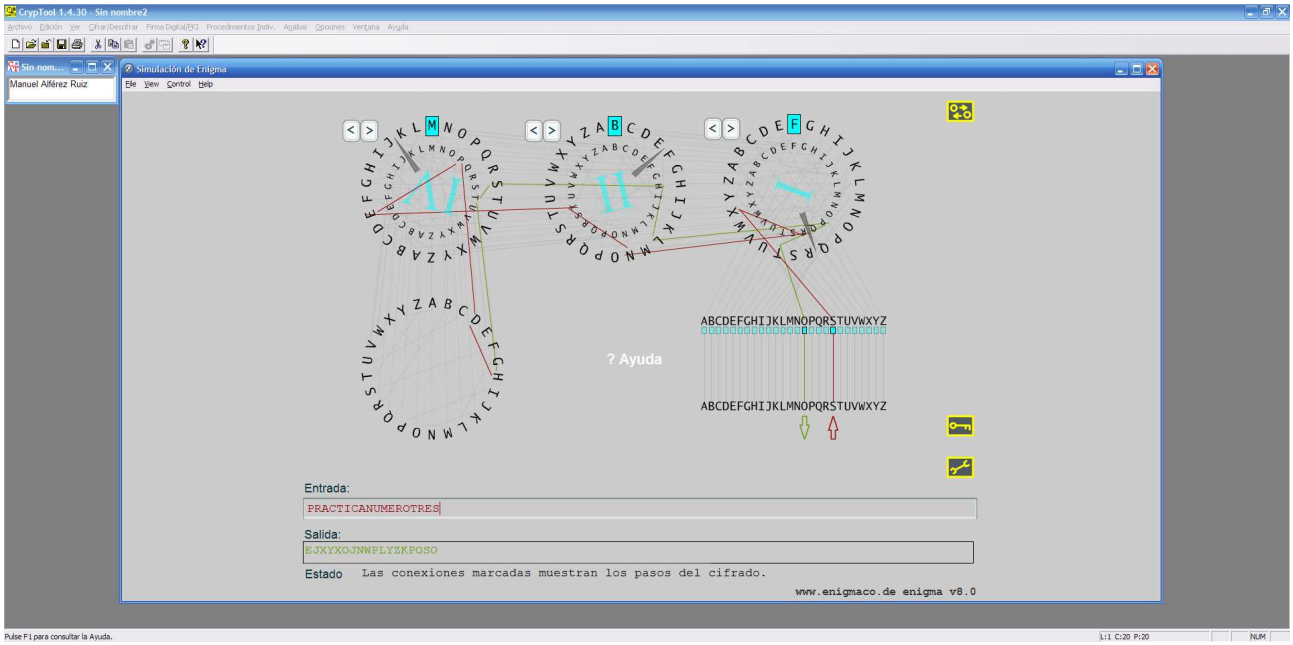
[5.png]

Una vez ajustado los rotores, debemos de disponer la *configuración inicial* con las tres primeras letras de mi nombre: Manuel= man.



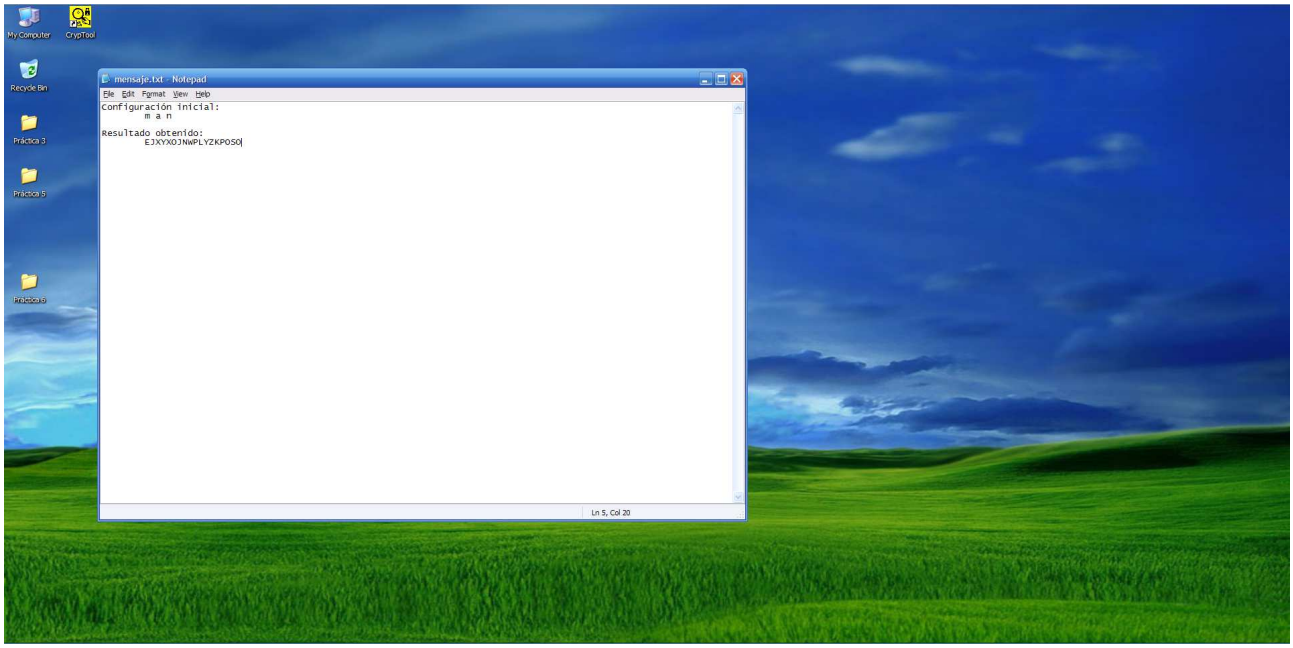
[6.png]

A continuación, escribimos el mensaje que deseamos cifrar: *PRACTICA NUMERO TRES*.



[7.png]

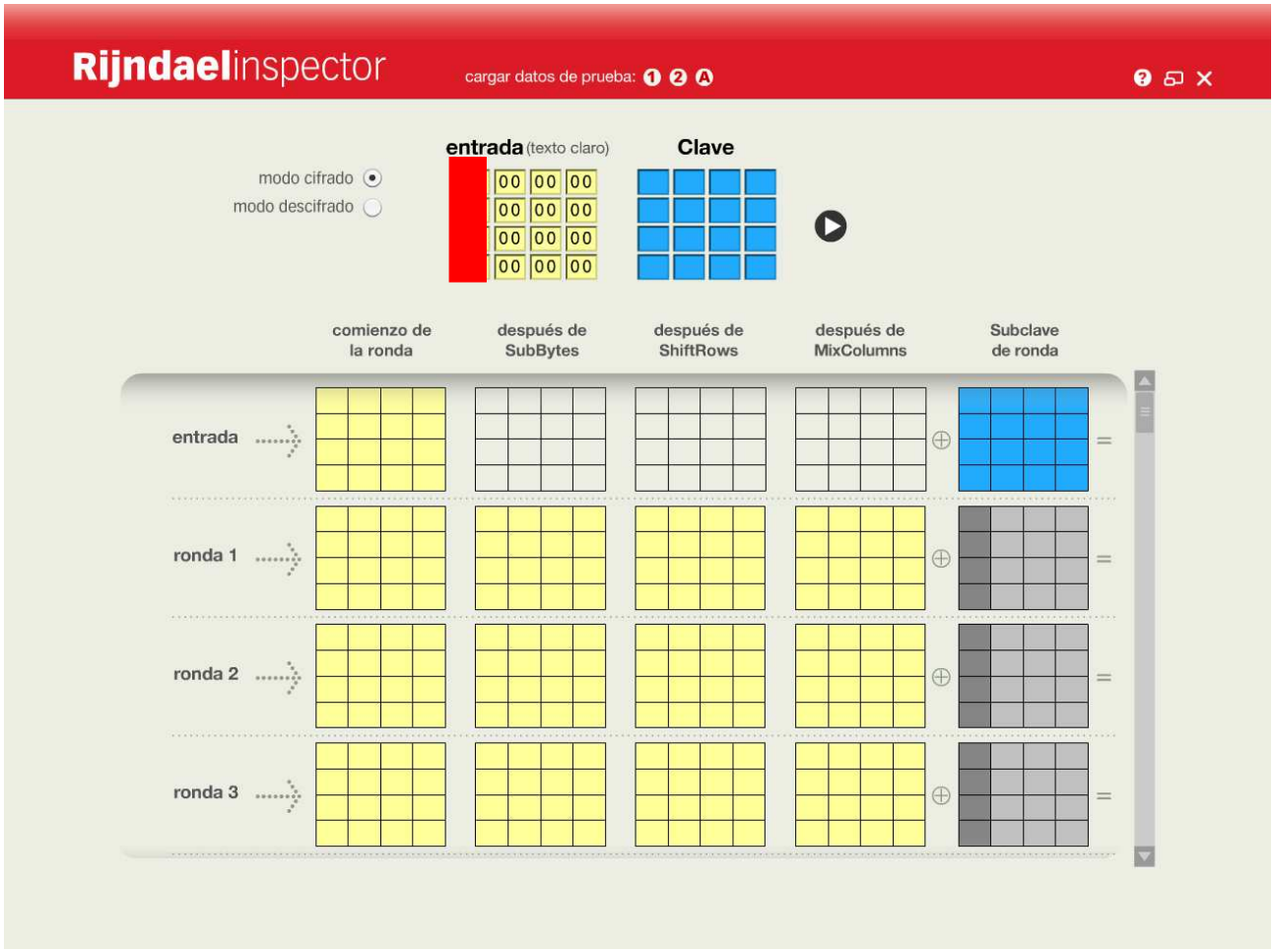
En última instancia, elaboramos un *documento de texto* con la información relativa a la configuración inicial y el resultado del mensaje ya cifrado:



[8.png]

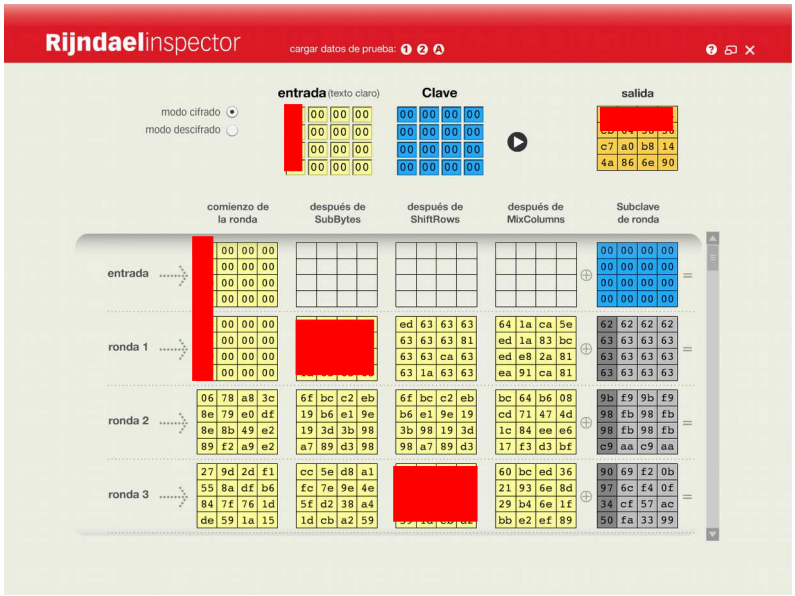
Cifrados modernos

En último lugar, vamos a cifrar los dígitos de mi *DNI* usando un cifrado moderno como es el *AES*. Debemos de colocar en la primera columna los dígitos de dos en dos:

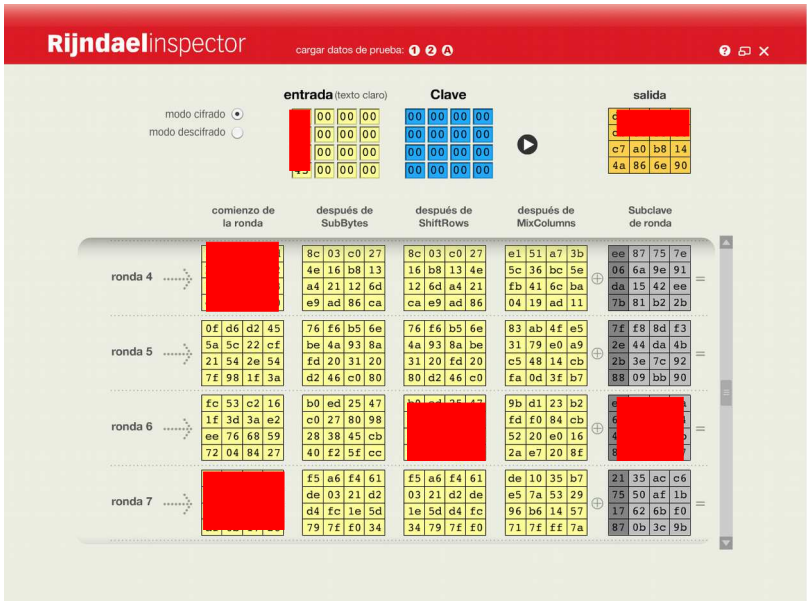


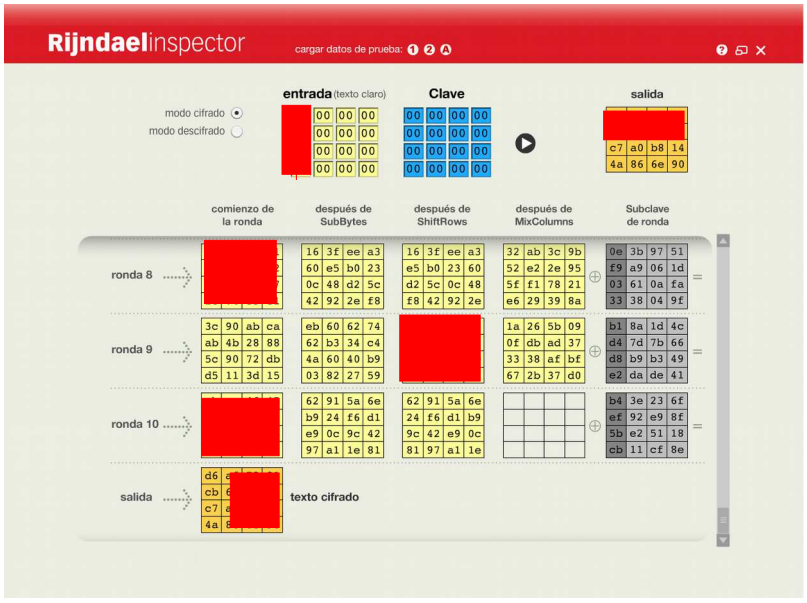
[9.png]

Como podemos ver las tres columnas restantes las rellenamos con ceros y pulsamos en ejecutar para que se genere la clave ya cifrada:



En la imagen podemos ver las tres primeras *rondas* del proceso que utiliza AES para cifrar el mensaje. A continuación las demás rondas hasta llegar a la salida final:





Los valores obtenidos los almacenamos en un documento de texto como en la sección anterior: