***Imagen que contiene Logotipo

Descripción generada automáticamente***

Alejandro Ortega Martínez

Grado en Ingeniería Informática

3/5/2021

Practica 3

Seguridad Informática

Contenido

[1. Cifradores de clave secreta 2](#_Toc72702328)

[1.1. Cifradores de clave secreta 2](#_Toc72702329)

[Apartado 1. Archivos de Texto 2](#_Toc72702330)

[Apartado 2: Archivos con formato 5](#_Toc72702331)

[Apartado 3: Archivos ejecutables 7](#_Toc72702332)

[Informe 9](#_Toc72702333)

[2. Cifradores de clave Publica 10](#_Toc72702334)

[2.1. Cifrador de mochila de Merkle-Hellman 10](#_Toc72702335)

[Apartado 1 10](#_Toc72702336)

[Apartado 2 15](#_Toc72702337)

[2.2. Cifrado RSA 23](#_Toc72702338)

[2.3. ElGamal 27](#_Toc72702339)

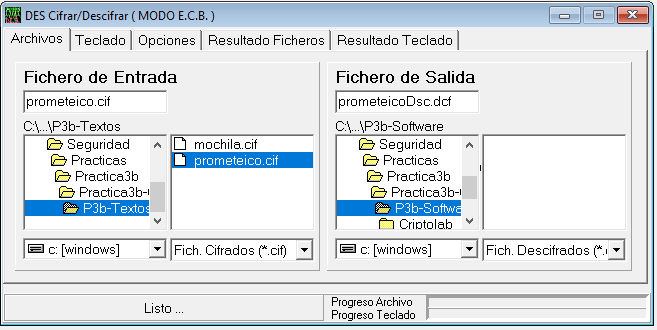
# 1. Cifradores de clave secreta

## 1.1. Cifradores de clave secreta

### Apartado 1. Archivos de Texto

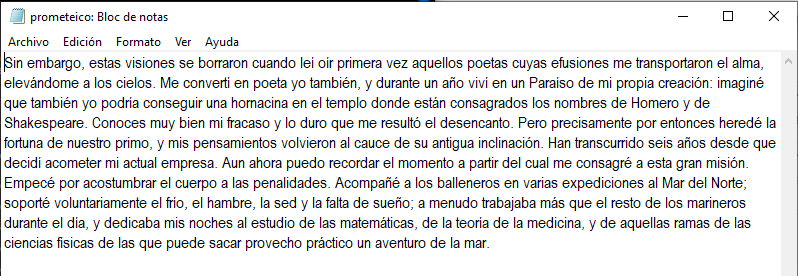
**a)Intente descifrar el fichero PROMETEICO.CIF llamando al fichero de salida PROMETEICO.DCF si nos han dicho que la clave puede ser cualquiera de las siguientes: ¿Franki?; Frankens; Prometeo; prometeo; 1234Mary; MaryShel; marymary. Se sabe que la cifra se ha realizado con el modo ECB.**

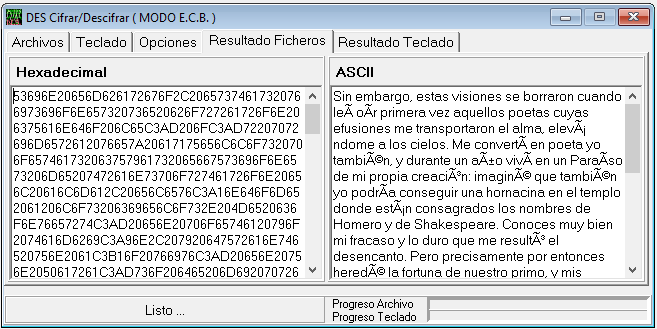
Para ello utilizaremos el safeDES.



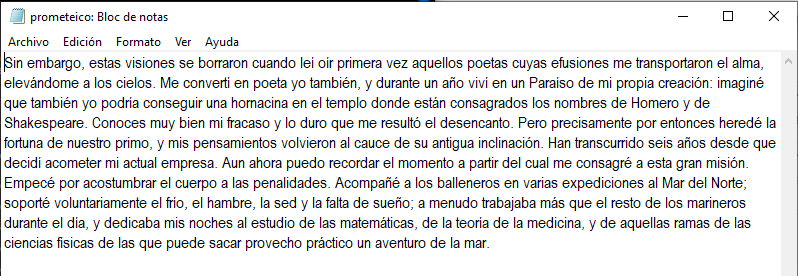


Utilizando la contraseña MaryShel, como se muestra previamente, conseguimos el siguiente resultado:



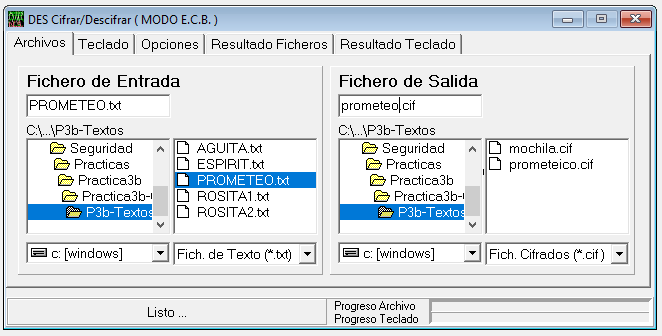
**b)Observe el fichero PROMETEICO.DCF en hexadecimal y su representación en forma de texto. Editelo luego con el Bloc de Notas.** 

AL abrirlo con el bloc de notas, nos deja editarlo cómodamente:

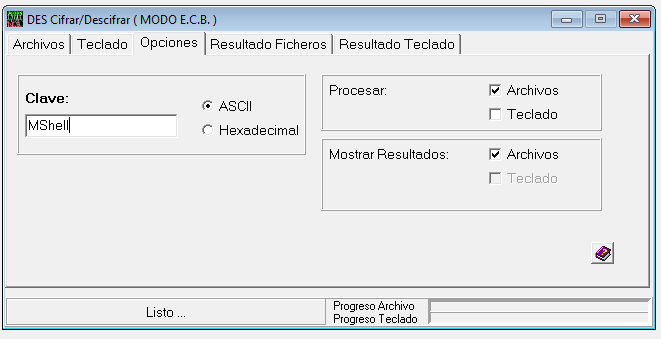
****

**c)Cifre el fichero PROMETEO.TXT con la clase K=MShelley y anote los 8 primeros caracteres en hexadecimal del criptograma.**

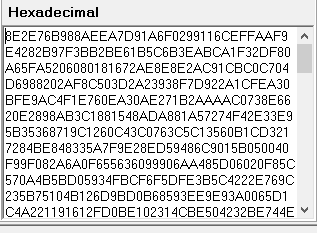
Seleccionamos los ficheros:



Introducimos la clave:



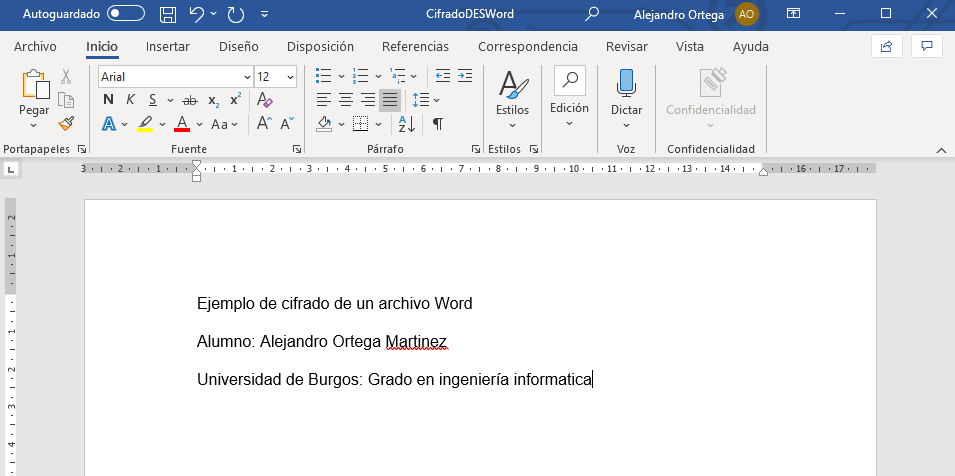
Anotamos los primeros caracteres: 8E2E76B9



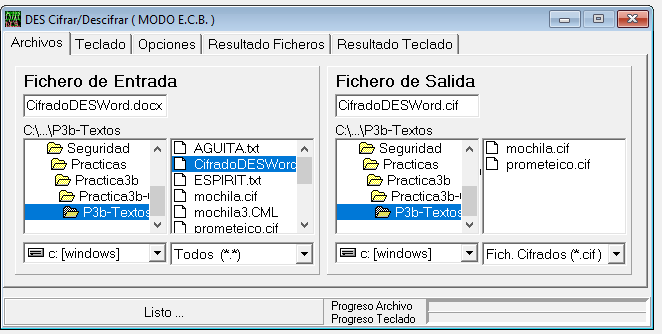
### Apartado 2: Archivos con formato

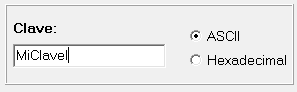
**a)Cree un documento cualquiera con Word, Wordperfect u otro programa de texto y cífrelo usando como clave K=MiClavel. El fichero cifrado se llamará igual que el original pero con extensión CIF.**

Creamos el documento:



Ahora lo ciframos con DES:

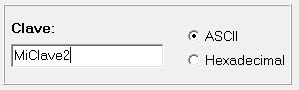




Y nos crea el siguiente archivo:

**b)Cifre ahora el mismo documento pero con la clave K=MiClave2. Llame al fichero cifrado con distinto nombre que el anterior pero con extensión CIF.**

Repetimos los pasos anteriores, pero cambiando la clave:

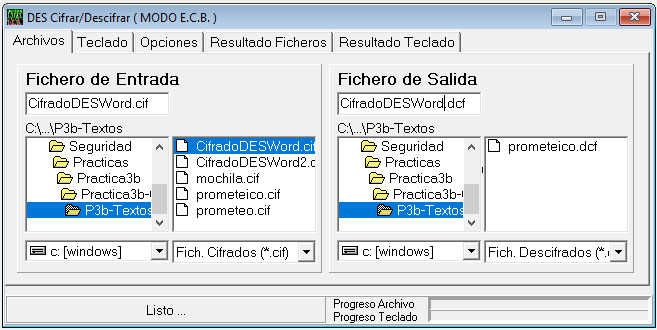


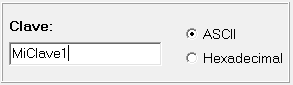
Y nos crea el siguiente archivo:



**c)Descifre ahora los criptogramas obtenidos llamando a los ficheros con su respectivo nombre y la extensión DCF.**

Desciframos primero el de la clave 1:

****

****

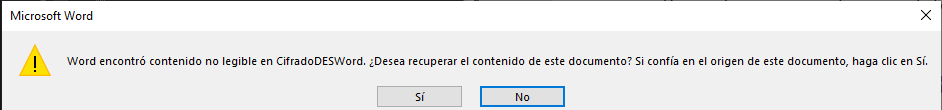
Hacemos lo mismo con la clave2, y nos genera los siguientes archivos:



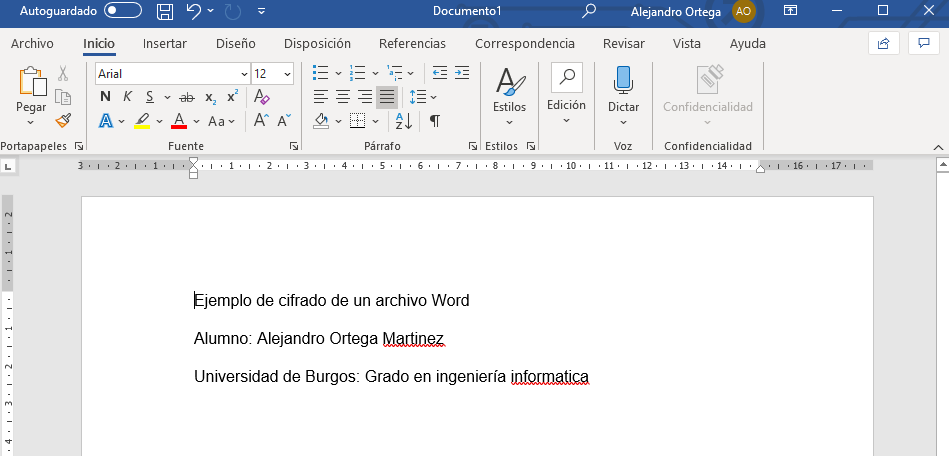


**d)Intente abrir los archivos cifrados anteriormente con el programa o aplicación que generó el fichero**

Primero tenemos que seleccionar el abrir con, para abrir los ficheros con Word, y nos dará el siguiente mensaje:



Si le damos a que si, nos abrirá dos documentos como el siguiente:

****

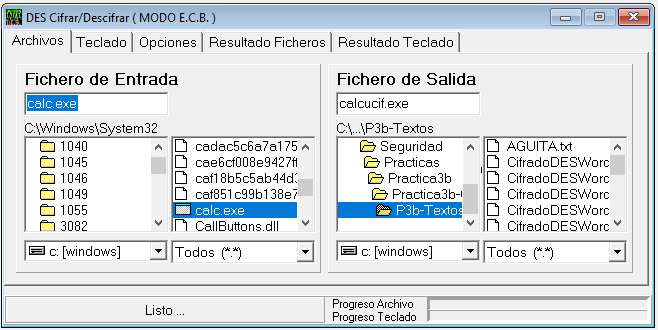
**e)Compruebe que los ficheros descifrados son idénticos a los ficheros.**

Como podemos observar en la captura del apartado anterior, los ficheros son idénticos.

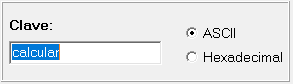
### Apartado 3: Archivos ejecutables

**a)Cifre el archivo CALC.EXE que encontrará en la carpeta C:\WINDOWS\SYSTEM32 con la clave K=calcular. Llame al fichero de salida CALCUCIF.EXE.**

Primero seleccionamos los archivos de entrada y de salida:

****

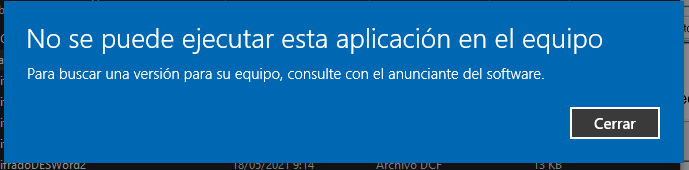
A continuación, seleccionaremos la clave:



Y nos crea el siguiente ejecutable:



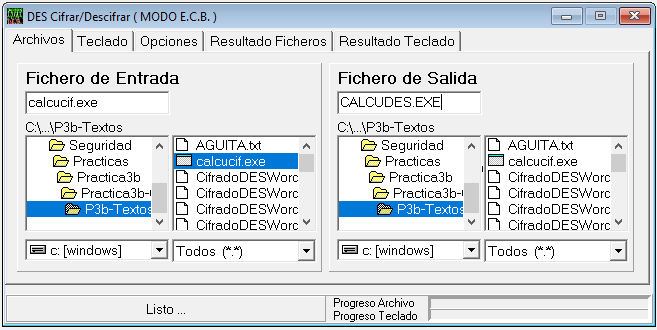
**b)Intente ejecutar el archivo CALCUCIF.EXE.**

****

Como podemos observar, Windows no nos deja ejecutar la aplicación.

**c)Descifre el archivo CALCUCIF.EXE llamándolo CALCUDES.EXE y compruebe que el archivo descifrado se ejecuta perfectamente.**

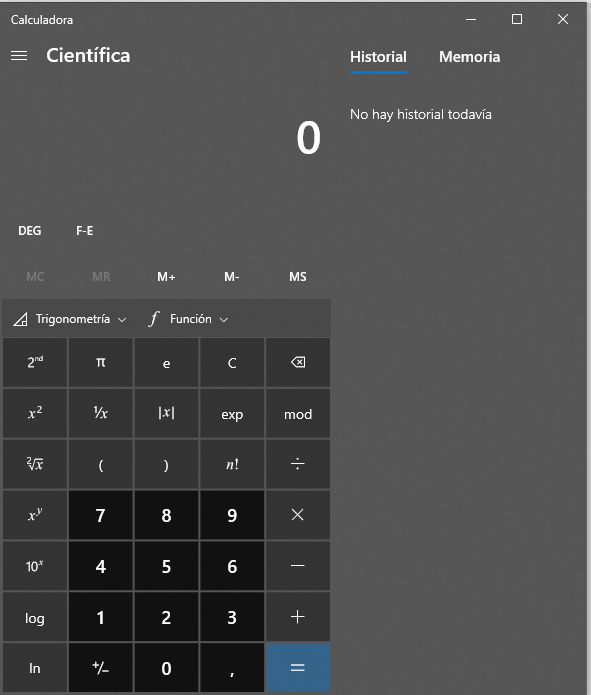
Lo desciframos como viene siendo habitual:



Y nos crea el siguiente ejecutable:



Al ejecutarlo, nos abre la calculadora:



### Informe

**1.¿Con qué clave ha podido descifrar el fichero del apartado 1?**

Se ha podido descifrar con MaryShel.

**2.¿Se corresponden los 8 primeros bytes en hexadecimal del texto recuperado en el apartado 1.c con los caracteres ASCII del texto en claro.**

Si, se corresponden.

**3.¿Le llama algo la atención los valores en hexadecimal del comienzo y del final de los ficheros con formato que se han cifrados con DES?**

Coinciden con los caracteres ASCII.

**4.Comente lo sucedido en el apartado 3. ¿Son exactamente iguales los ficheros CALC.EXE y CALCUDES.EXE.**

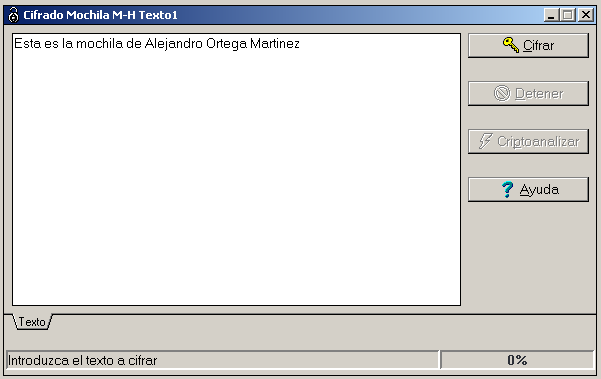
Se ha podido ejecutar con total normalidad.

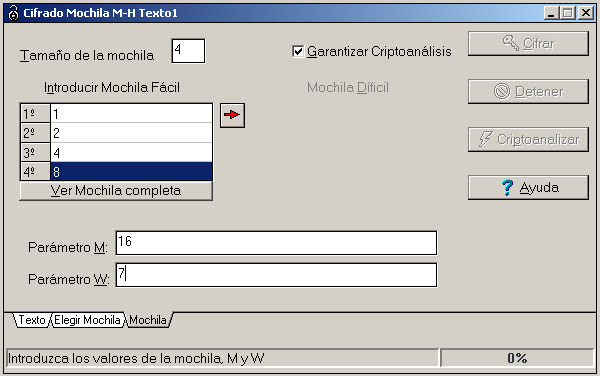
# 2. Cifradores de clave Publica

## 2.1. Cifrador de mochila de Merkle-Hellman

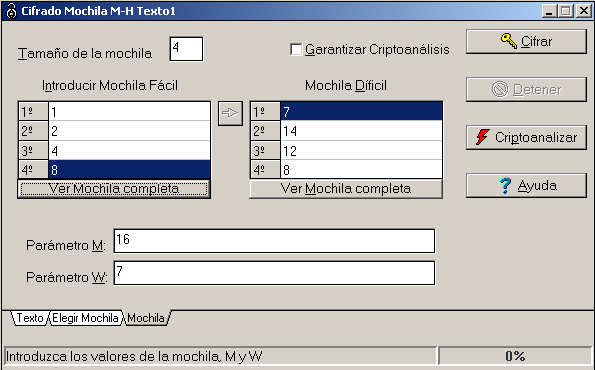
### Apartado 1

**a)Cifre el mensaje M = “Esta es la mochila de <Nombre\_Alumno/s>”, usando la mochila simple [1,2,4,8] con u=16 y w=7.**

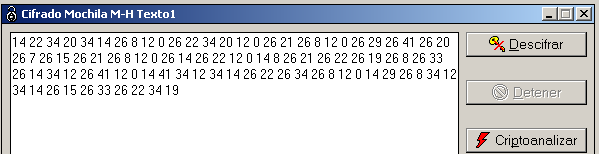
****

****

Despues de esto nos calcula la “Mochila dificil”, que es la clave publica

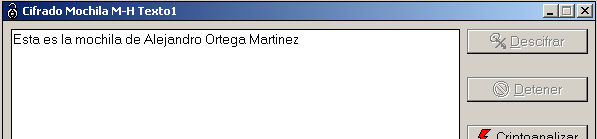


El texto cifrado es el siguiente:



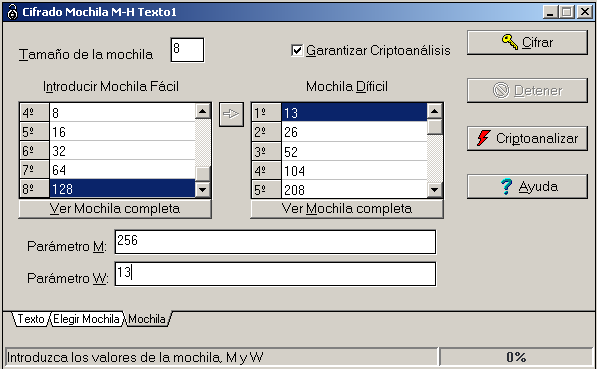
**b)Descifre el criptograma anterior.**

Dándole al botón de arriba a la derecha, donde pone descifrar, obtenemos el mensaje descifrado:

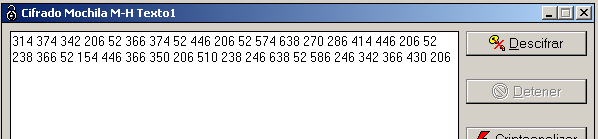


**c)Con la mochila simple [1,2.4,8,16,32,64,128], u=256 y w=13, repita la cifra del punto a).**

Siguiendo la metodología anterior, hacemos:

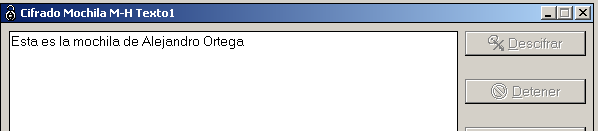
****

El resultado es el siguiente:

****

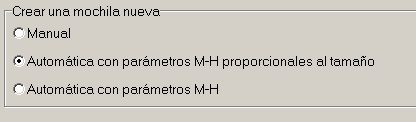
**d)Descifre el criptograma anterior.**

Siguiendo las instrucciones del apartado b), obtenemos:



**e)Cifre el mensaje M=”Errar es humano, usando la mochila de <Nombre\_Alumno/s>” con valores de Merkle-Hellman proporcionales de tamaño n=15, garantizando el criptoanálisis. Anote la mochila fácil, la mochila difícil y sus parámetros.**

Para ello, seleccionamos la opción:



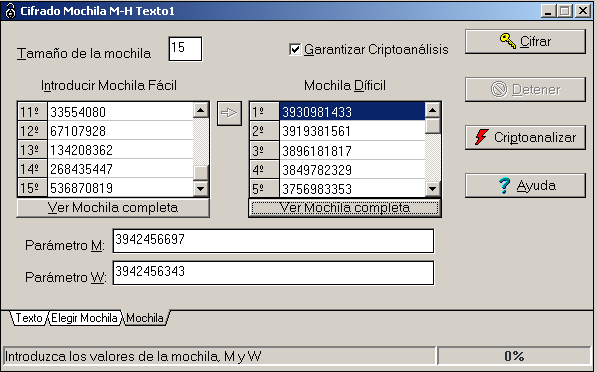
Como podemos observar, nos ha generado los siguientes parámetros:

Mochila Simple=[32416, 65184, 130720, 261792, 523936, 1048224, 2096800, 4193952, 8388256, 16776864, 33554080, 67107928, 134208362, 268435447, 536870819]

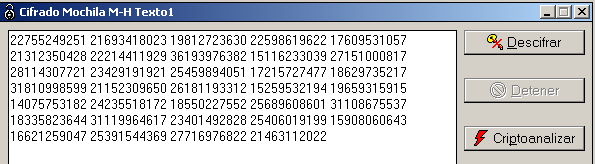
M=3942456697

W=3942456343

Mochila Difícil=[3930981433, 3919381561, 38961817, 3849782329, 3756983353, 3571385401, 3200189497, 2457797689, 973014073, 1945903538, 3891682468, 3840990367, 3742176913, 3535269187, 3128108227]

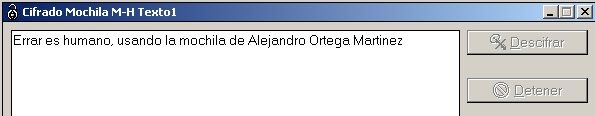


El criptograma nos queda así:

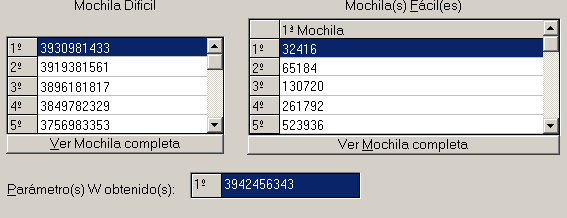


**f)Descifre y criptoanalice el criptograma anterior.**

Si le damos a descifrar, nos queda lo siguiente:



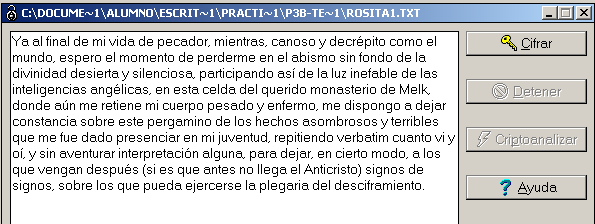
Y criptoanalizando (criptoanálisis rapido), obtenemos el siguiente resultado:

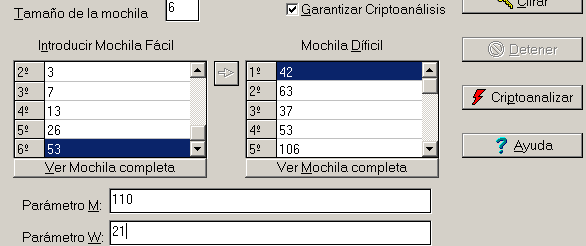


### Apartado 2

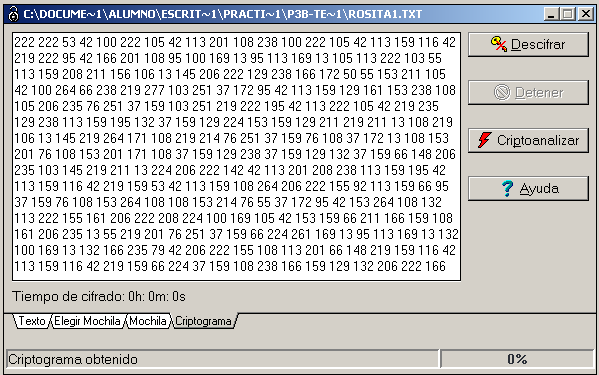
**a)Cifre el fichero ROSITA1.TXT usando la mochila simple [2,3,7,13,26,53] con u=110 y w=21. El fichero de salida se llamará ROSITA1.CIF.**

Para cifrar ficheros, damos click derecho en la ventana en la que introducimos el texto, y seleccionamos fichero, ahí, elegimos el fichero deseado:

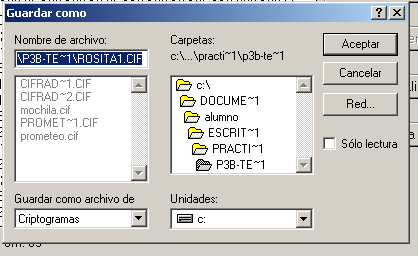
introduciendo los datos, nos quedan los siguientes parámetros:



A la hora de cifrarlo, obtenemos el siguiente resultado:

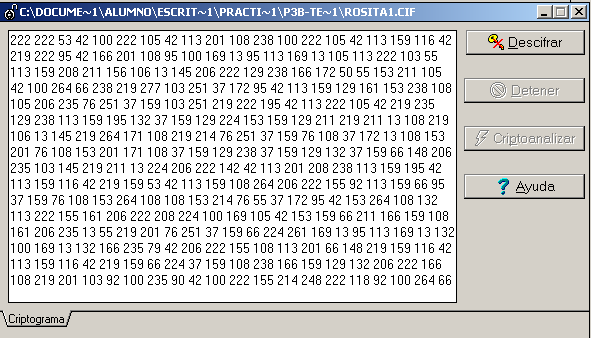


Para guardar, damos click derecho en el criptograma y seleccionamos “Salvar criptograma”

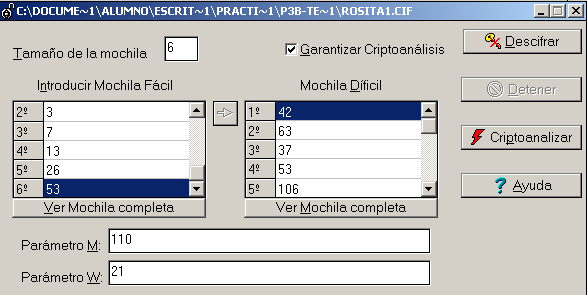


**b)Descifre el fichero ROSITA1.CIF, guardándolo como ROSITA1.DCF.**

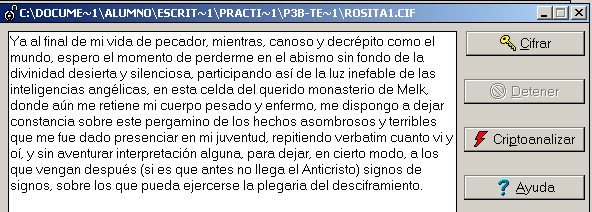
Primero seleccionamos la ventana de descifrar, click derecho, y seleccionamos nuestro fichero, que se quedara así:



A continuación le daremos a manual, e introduciremos los parámetros públicos para descifrar, que son los dados en el enunciado anterior, que es la clave publica:

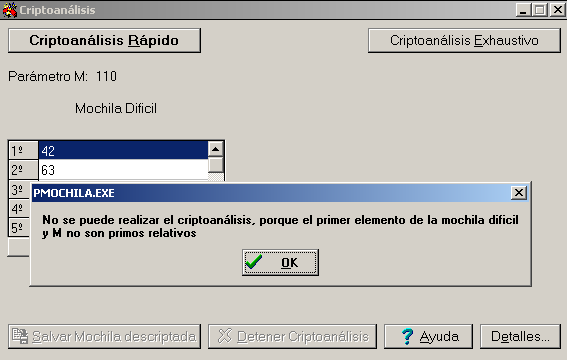


Si le damos a descifrar, nos saldrá el texto original:



Para guardarlo, seguiremos los mismos pasos explicados anteriormente.

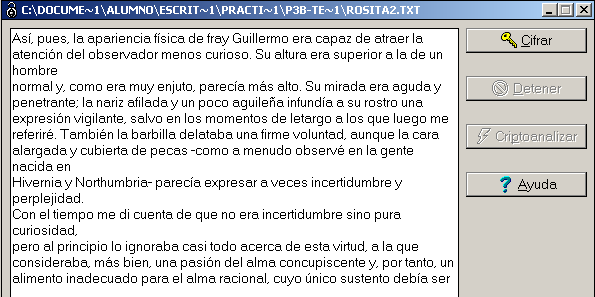
**c)Intente criptoanalizar el fichero ROSITA1.CIF.**

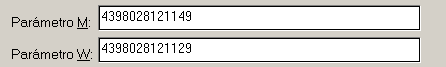
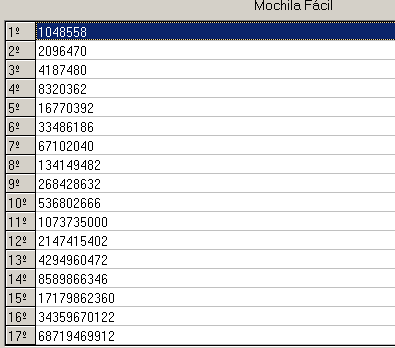


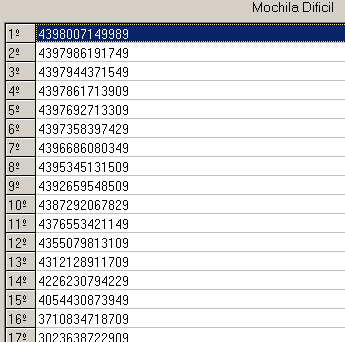
Como podemos observar, no se puede criptoanalizar.

**d)Cifre el fichero ROSITA2.TXT usando una mochila de Merkle-Hellman con valores proporcionales a n=20. Anote la mochila fácil, la mochila difícil y sus parámetros propios. Asegúrese de tener activada la posibilidad de criptoanálisis. El fichero de salida llamará ROSITA2.CIF.**

Para cifrarlo, seguiremos los pasos vistos en el anterior apartado de cifra con valores proporcionales, que son los siguiente:



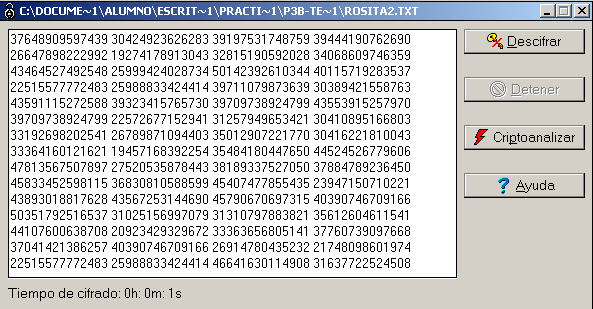






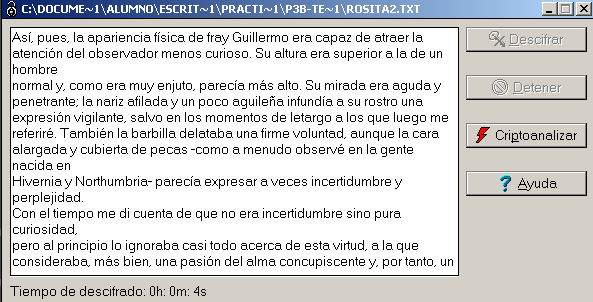


El fichero cifrado tiene la siguiente forma:

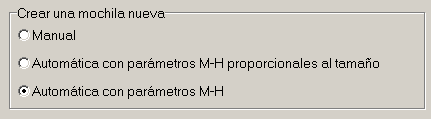


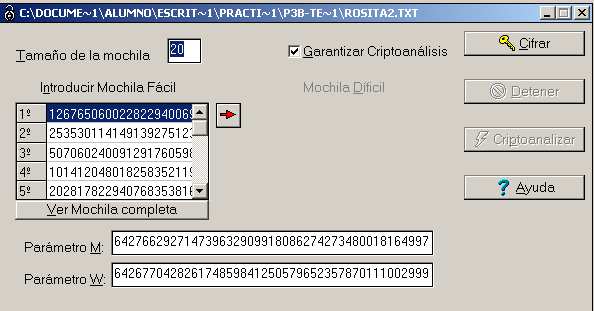
**e)Descifrar el fichero ROSITA2.CIF, guardándolo como ROSITA2.DCF.**

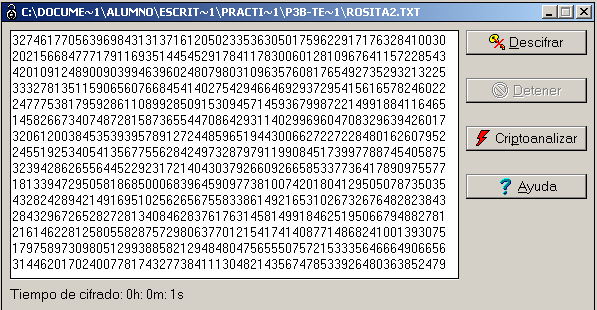
Siguiendo los pasos que hemos visto anteriormente para descifrar ficheros, obtenemos el siguiente resultado:



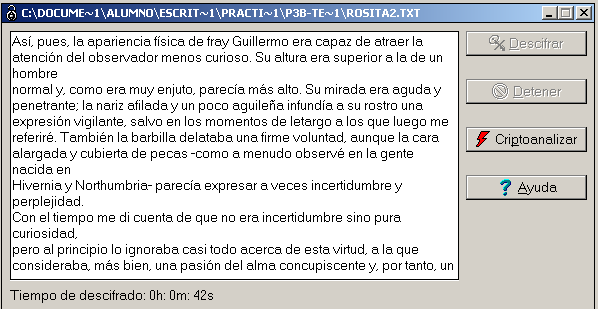
**f)Vuelva a cifrar el fichero ROSITA2.TXT usando ahora una mochila de Merkle-Hellman no proporcional con n=20. Descifre el criptograma y compare el resultado con el fichero recuperado anteriormente ROSITA2.DCF.**

****

****

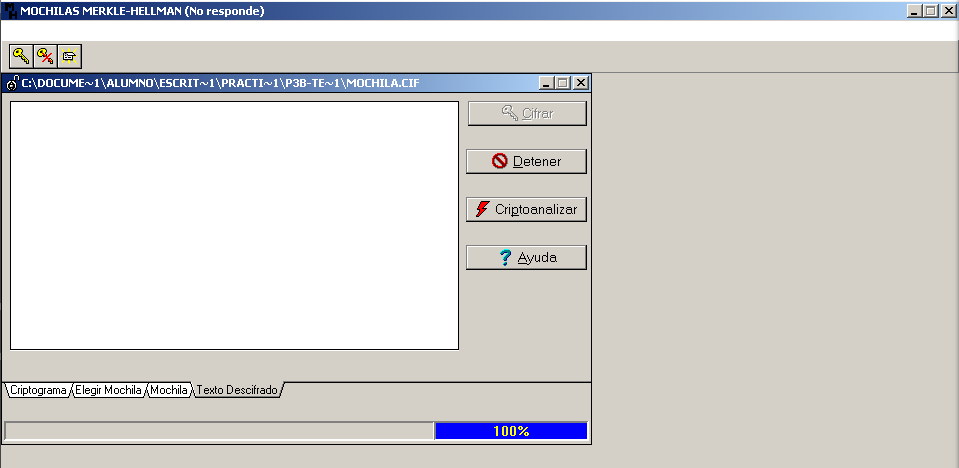
****

Si lo desciframos, obtenemos el siguiente resultado:



**g)Descifre el fichero MOCHILA.CIF (o MOCHILA3.CML si se usa CriptoMiniLab), si se sabe que ha sido cifrado con alguna de estas tres mochilas de Merkle-Hellman: [23,47,111,239,495] u=4005, w=3994; [29,61,125,253,509] u=3748, w=3743; [26,64,122,256,506] u=4015, w=3198. ¿De qué archivo se trata?**

Nota: No he conseguido descifrarlo, ya que cada vez que lo intento, la aplicación deja de responder:



#### Informe

**1.Comente los resultados obtenidos en el apartado 1. ¿Es una buena opción elegir mochilas de tamaño 8 o de tamaño 4?**

Podemos ver que cuanto mas grande es la mochila, mas seguro es el cifrado, por lo que el usar mochilas tan pequeñas, como de tamaño 4 u 8, puede ser mala idea.

**2.Compruebe teóricamente los dos primeros valores del criptograma obtenido en el apartado 2a.**

Tenemos la mochila simple {2,3,7,13,26,53}

De la cual sacamos la mochila Difícil {42, 63, 37, 53, 106, 13}

El primer carácter es una Y, que en código ascii es 89. Esto, pasado a binario, es 01011001

Cogemos los primeros 6 bits, ya que nuestra mochila es de tamaño 6, y son: 010110.

Ahora, multiplicamos cada uno por su posicion en la mochila:

0\*42 + 1\*63 + 0\*37 + 1\*53 + 1\*106 + 0\*13 = **222**

Vemos que, en efecto, es lo que nos daba el resultado.

Lo mismo ocurre con el segundo valor.

**3.¿Qué puede decir de los valores de las mochilas fácil y difícil generadas en los apartados 2d y 2f?**

Los valores que se generan con mochilas proporcionales son mucho menores que los generados con mochilas no proporcionales.

Debido a esto, es más seguro una encriptación con una mochila no proporcional, que con una mochila proporcional.

**4.¿Qué sucede si en el apartado 2g modifica algún valor de la mochila de cifra encontrada?.**

No se ha podido realizar el apartado g

## 2.2. Cifrado RSA

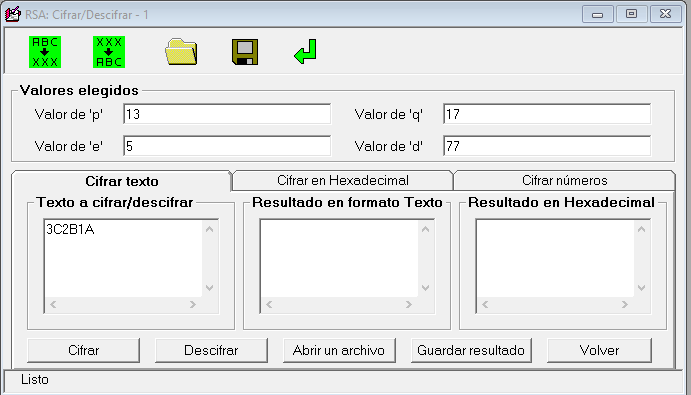
#### Apartado 1

**a)Con p=11, q=13 y e=1 cifre el mensaje M=OLA.**

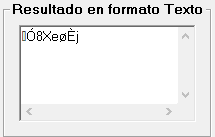
El valor e no puede ser 1, porque el exponente al 1 no cifraría nada.

**b)Con p=13, q=17 y e=5 cifre el mensaje M=3C2B1A.**

Realizaremos el cifrado con expocript:

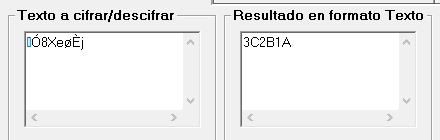


El cifrado nos da lo siguiente:

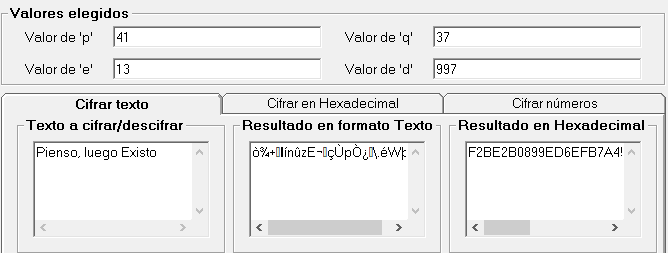


**c)Descifre el criptograma del punto anterior.**

Ponemos el texto anterior en texto a descifrar, y le damos a descifrar con los mismos parámetros, obteniendo lo siguiente:

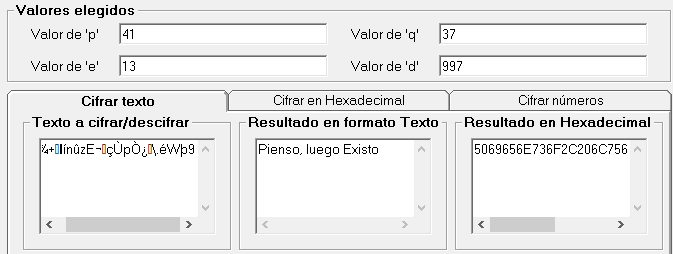


**d)Con p=41, q=37 y e=13, cifre el mensaje M=Pienso, luego existo.**

****

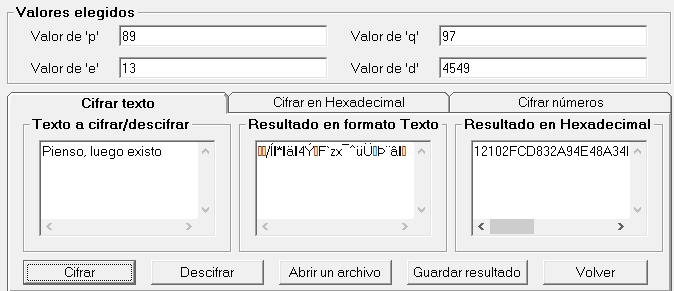
**e)Descifre el criptograma del punto anterior.**

Seleccionando la opción de descifrar, y poniendo el resultado cifrado obtenido anteriormente en el campo del texto a descifrar, obtenemos lo siguiente:

****

**f)Repita la cifra del punto d) usando ahora los primos p=89 y q=97.**

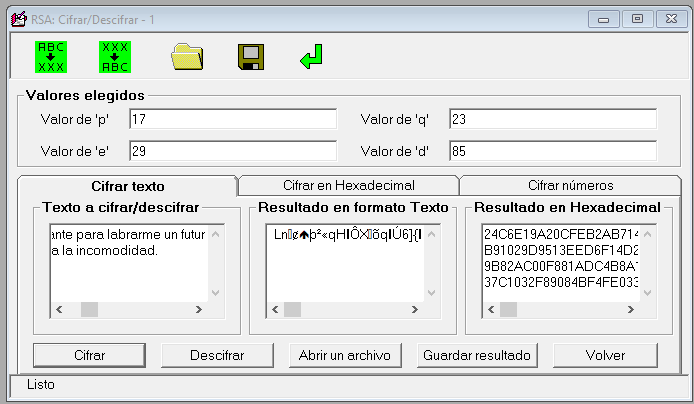
Metiendo los nuevos valores, obtenemos el siguiente resultado:



#### Apartado 2

**a)Cifre con los valores p=17, q=23 y e=29 el fichero ESPIRIT.TXT. El fichero de salida se llamará ESPIRIT.CIF..**

Despues de un buen rato cifrando, tenemos el siguiente resultado:

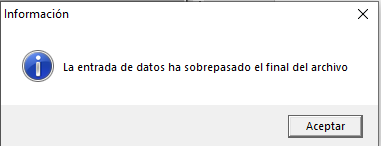


Para guardar el archivo, seleccionamos guardar resultado:



**b)Descifre el fichero ESPIRIT.CIF guardándolo como ESPIRIT.DCF..**

Realizamos el proceso inverso al del anterior apartado:



Nos sale el siguiente mensaje, indicando que el archivo cifrado es demasiado grande, pero el proceso seria similar al anterior.

#### Informe

**1.Explique y justifique qué ha sucedido en la cifra del punto 1a.**

No nos ha dejado encriptar, ya que siendo el exponente 1, el mensaje encriptado seria igual que el original, y el programa, por seguridad, no permite hacerlo.

**2.Compruebe los valores de cifra y descifrado del mensaje del apartado 1b.**

**3.¿Podría cifrar cualquier mensaje en ANSI con el grupo del apartado 1a?**

Si, pero se quedarían igual.

**4.Compruebe la cifra y el descifrado de los dos primeros bytes del fichero ESPIRIT.TXT del apartado 2a.**

**5.Si tuviera que elegir un sistema de cifra, ¿elegiría este sistema RSA en el que se cifra el mensaje por bytes? ¿Por qué?**

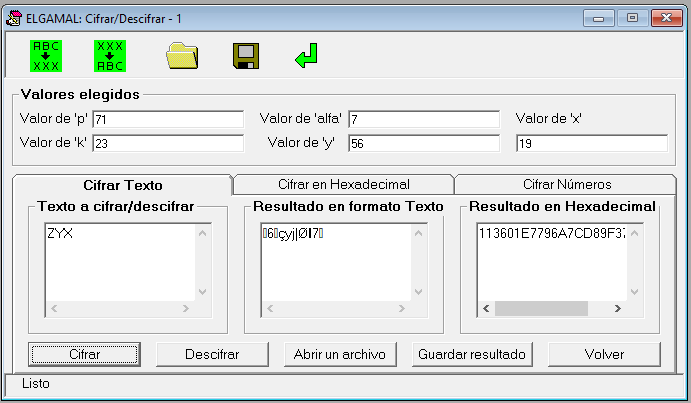
Si, porque es mucho mas seguro que el sistema de mochila, ya que el algoritmo de la mochila es mucho mas facil de romper, mientras que este es mas seguro matemáticamente hablando.

## 2.3. ElGamal

#### Apartado 1

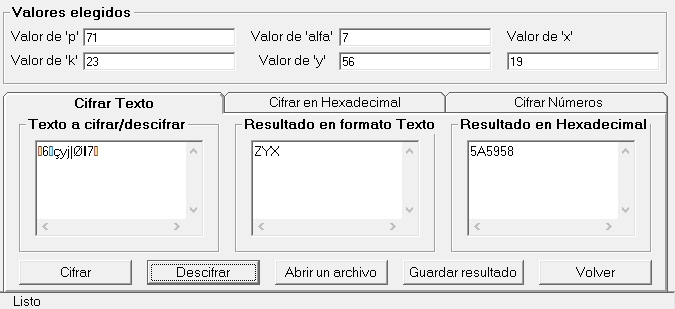
**a)Con p=71, alfa=7, v=19 y b=23 cifre el mensaje M=ZYX.**

Utilizando también el expocript, de manera análoga al cifrado RSA, tenemos:



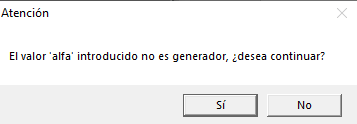
**b)Descifre el criptograma del punto anterior.**

Para descifrar hacemos algo similar. Ponemos el criptograma en la casilla de texto a descifrar, y con los mismos parámetros, le damos a descifrar

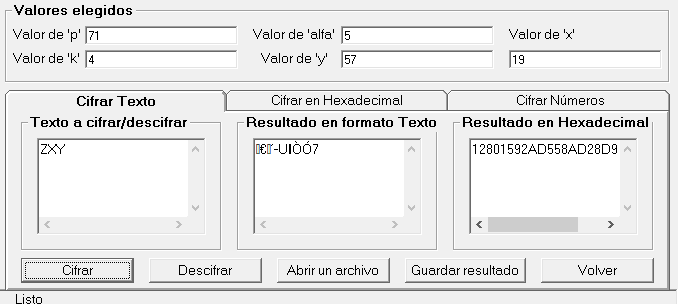


**c)Si ahora alfa=5, repita la cifra del punto 1a para b=4 y b=9.**

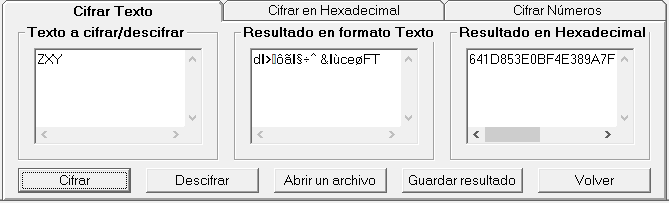
Nos dice que el valor alfa no es generador, pero continuaremos igualmente:



Hacemos la cifra para alfa=5 y b=4



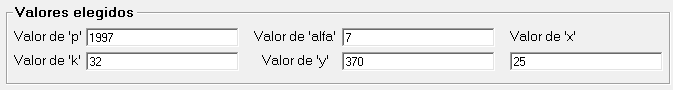
Ahora probaremos con alfa=5 y b=9



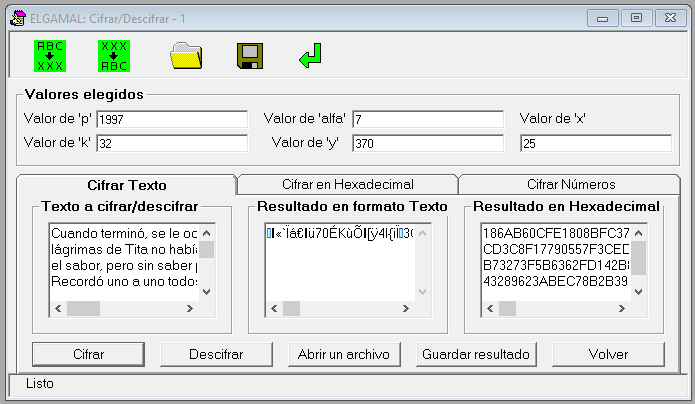
#### Apartado 2

**a)Con p=1997, a =7, v=25 y b=32 cifre el fichero AGUITA.TXT. El fichero de salida se llamará AGUITA.CIF.**

Iniciamos la encriptación con los siguientes valores:



Para cargar ficheros, se hace de la misma manera que con el cifrado RSA, por lo que, una vez cifrado, nos queda de la siguiente manera:



Por ultimo, lo guardaremos en un archivo



**b)Descifre el fichero AGUITA.CIF, guardándolo como AGUITA.DCF.**

Realizando el proceso contrario, tenemos:

NOTA: El archivo es demasiado grande para descifrarlo (el programa da error), pero el procedimiento sería igual.

#### Informe

**1.Compruebe la cifra y el descifrado del mensaje del apartado 1a.**

Z en ascii es 90

719 mod 771 = 56.

723 mod 71 = 53.

90\*5623mod 71 = 42.

Cifra (31, 54)

Descifrado

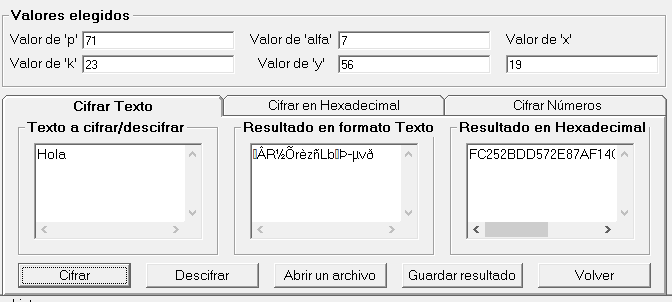
5319mod 71 = 62

42 \* inv(62, 72) = 63

63 mod 71 = 90 **Se verifica**

**2.¿Podría cifrar con los parámetros del apartado 1a el mensaje M=Hola?**

Si, como se muestra a continuación:



**3.¿Qué puede decir de los criptogramas encontrados en el apartado 1c?**

Que el valor alfa=5 no es generador.

**4.Compruebe la cifra y el descifrado de los dos primeros bytes del fichero AGUITA.TXT del apartado 2a.**

La metodología es similar al ejercicio 1, por lo que no se va a repetir.

**5.En general, ¿puede usar cualquier valor del CRR(p) como generador a?**

Tienen que ser raíz primitiva del espacio.