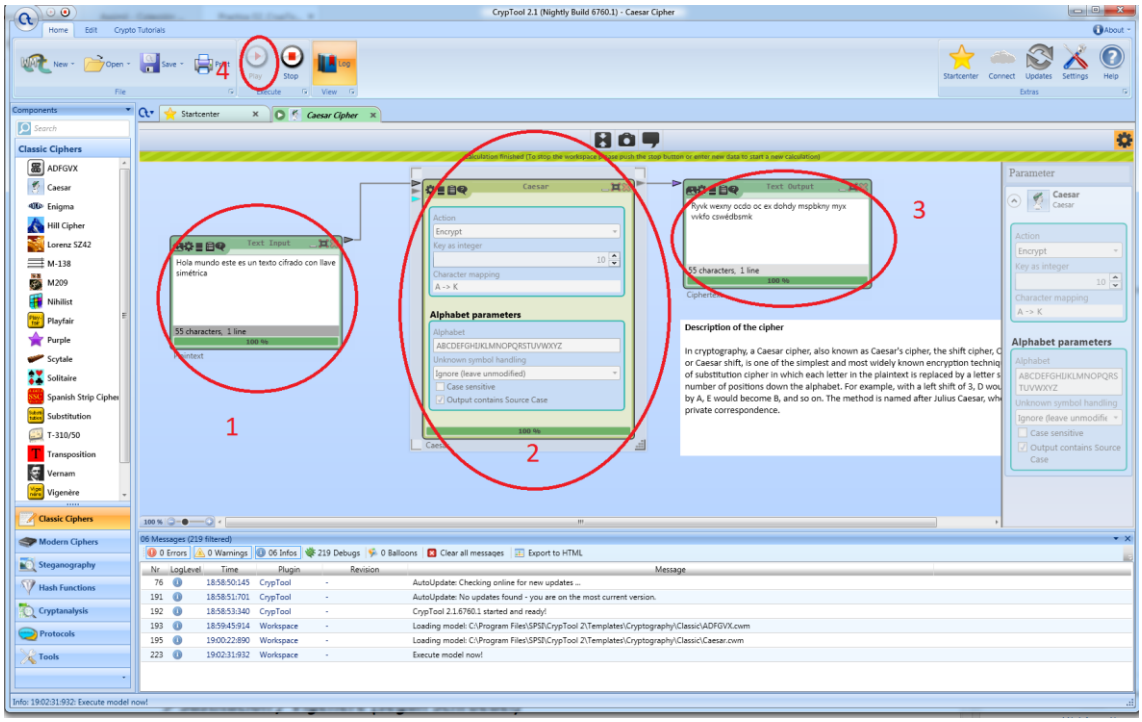
PRÁCTICA 2. CRYPTOOL.

4.

Cifrado César



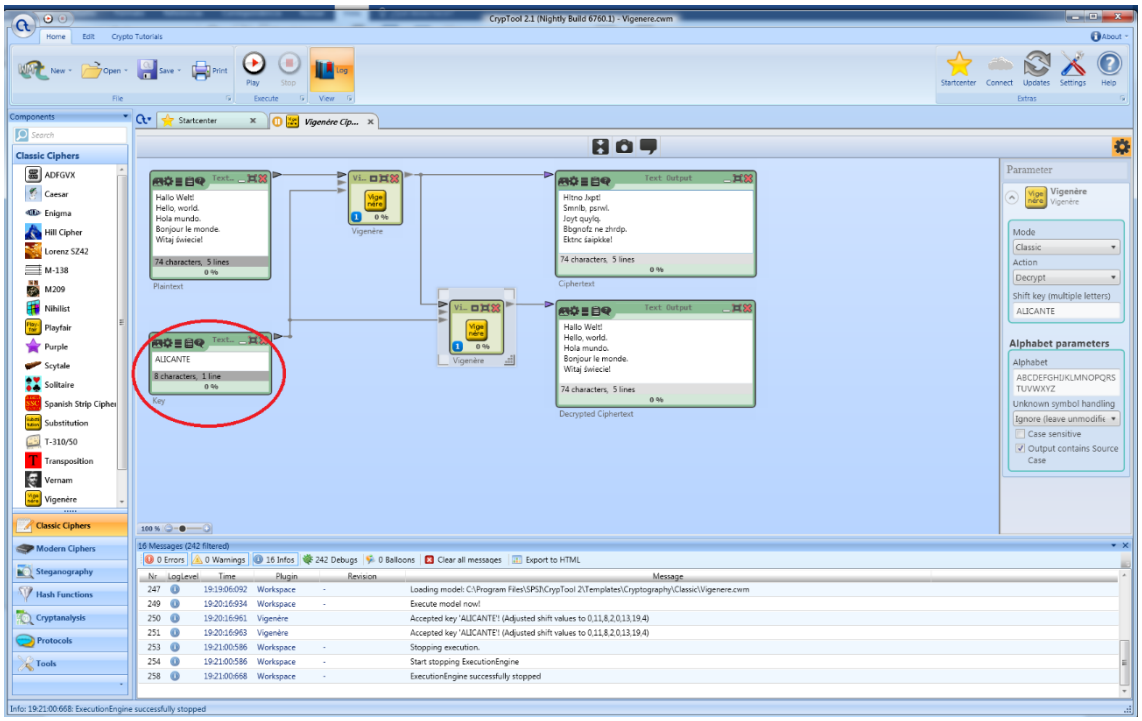
1. Entrada de texto. Texto que deseamos cifrar.
2. Parámetros del algoritmo. En este caso al ser César elegimos la clave k como 10.
3. Salida texto cifrado. Resultado de aplicar el algoritmo al texto de entrada.
4. Botón inicio. Para que se ejecute el algoritmo.

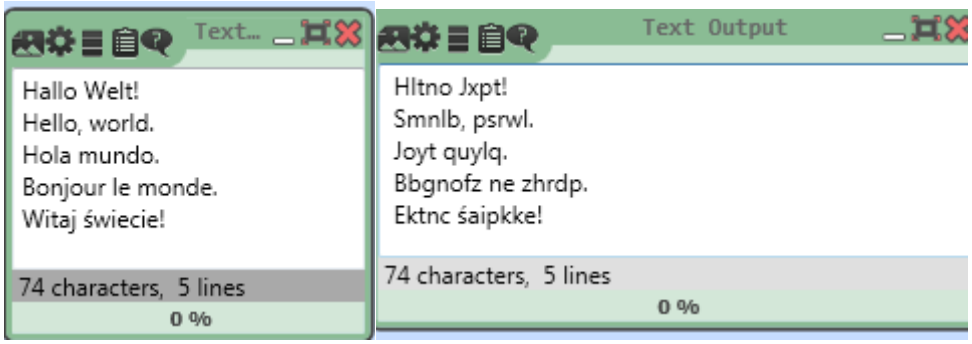
Explicación:

El algoritmo de César utiliza una función del conjunto de funciones que forman el sistema, en este caso 26, basado en la llave empleada. Por lo tanto, sería f(k) = i + k (mod 26) con i siendo el valor de la letra. El conjunto del mensaje y del cifrado, M y C, tienen cardinalidad 26.

Un ejemplo de este algoritmo con k=10 hace que A se transforme en K. La letra A=1 con la llave siendo 10 da como resultado la letra K=11(K = A +10)

CIFRADO VIGENERE





Descripción:

Este caso es un cifrado por sustitución polialfabético. La clave usada para el cifrado es la palabra ALICANTE, haciendo que, según la posición de la letra se aplique una función de cifrado distinta dentro de las 26 posibles. Las funciones son de la forma f(k,i)= i + k (mód 26) en la cual i es el valor de la letra según su posición en el abecedario, estando comprendido entre 0 y 25 y *k* el valor de la llave que se representa mediante una letra de la palabra clave. Por lo tanto, la llave elige una función, a la que se le pasa el valor de la letra a cifrar, *i*.

Para entenderlo mejor, podemos usar un ejemplo. Si miramos la primera palabra que se va a transformar "*Hallo*" vemos que la H se convierte en H, ya que la clave es A y el valor de k en la función al ser la primera letra del abecedario es 0, por lo tanto, la transformación es la identidad. La segunda letra a cifrar es la *a* y vemos que se convierte en *l*(ele), para ello la función usada es i+11(mod 26) siendo 11 la posición -1 dentro del abecedario de la letra *l.* Como a es 0, 0+11 = 11 y la letra devuelta es la l. En el tercer caso la función elegida es f(8,i)=i + 8(mod 26), que para i=11(letra ele), f(8,11) = 19(mod 26) que equivale a la letra *t*.

CIFRADO ADFGVX

Explicación:

Este es un algoritmo que usa sustitución y trasposición. Para ver cómo funciona empezamos con una matriz 6x6, donde colocamos las letras de la palabra clave, en este caso STAR WARS, yendo fila a fila sin repetir ninguna letra. Una vez colocado STARW colocamos el resto de letras que faltan del abecedario en orden alfabético A,B,C… y después los números del 0 al 9. En este caso faltan B,C,…,Q,U,V,X,Y,Z,0,…9.

	A	D	F	G	V	X
A	S	T	A	R	W	B
D	C	D	E	F	G	H
F	I	J	K	L	M	N
G	O	P	Q	U	V	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

Ciframos el texto *hola* con esta primera matriz buscando la letra a cifrar y transformándola en la pareja de letras (letra fila, letra columna), por ejemplo, la letra A se encuentra en la fila A y columna F, por lo tanto, el cifrado primero es AF.

Una vez cifrado el texto, tenemos que hacer una trasposición de las letras. Esto se hace mediante otra matriz que tiene como número de columnas el tamaño de la clave de trasposición. En este ejemplo usamos HAUS, y colocamos cada letra del texto cifrado por filas.

H	A	U	S
D	X	G	A
F	G	A	F

Ahora la trasposición consiste en ordenar las columnas en orden alfabético basándose en la palabra clave, pasando de HAUS a AHSU.

H	A	U	S
X	D	A	G

G	F	F	A

Finalmente, el texto cifrado es leyendo las columnas y agrupándolas en parejas.

Texto cifrado: XG DF AF GA

Clave usada: STARWS; clave trasposición: HAUS

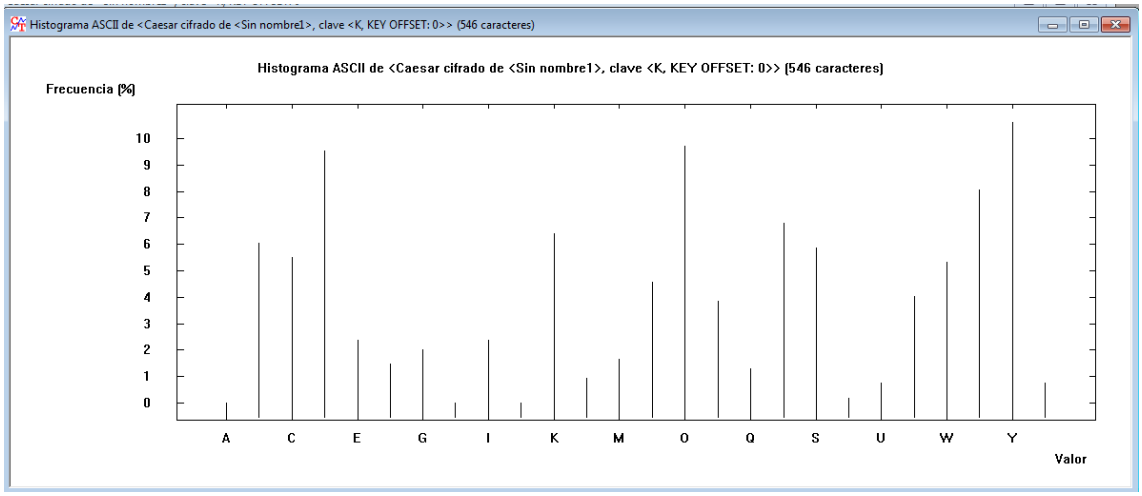
Análisis de los algoritmos:

Para realizar los estudios se ha utilizado el poema "*Alone*" de E.A.Poe.

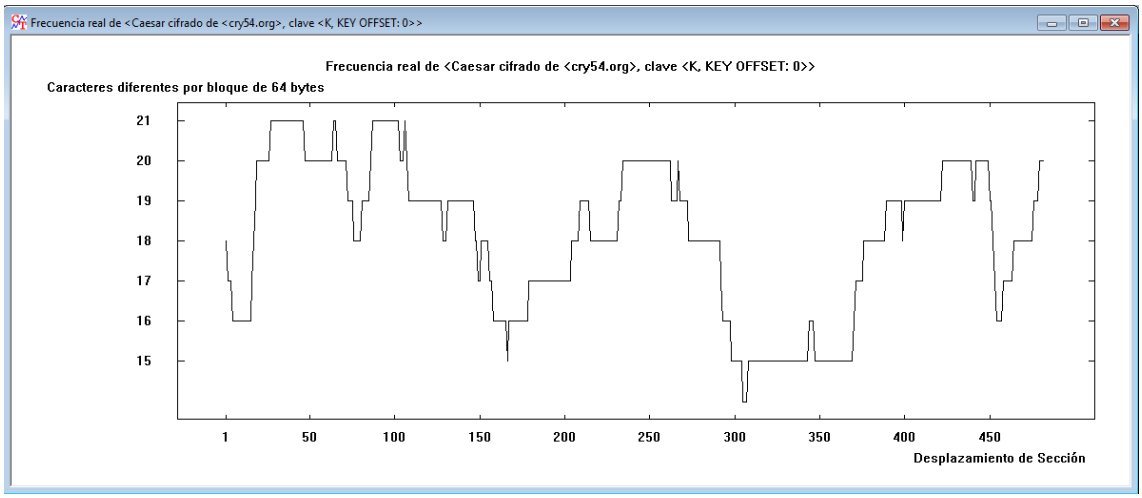
<u>César(clave k=K)</u>

Entropía = 4.13

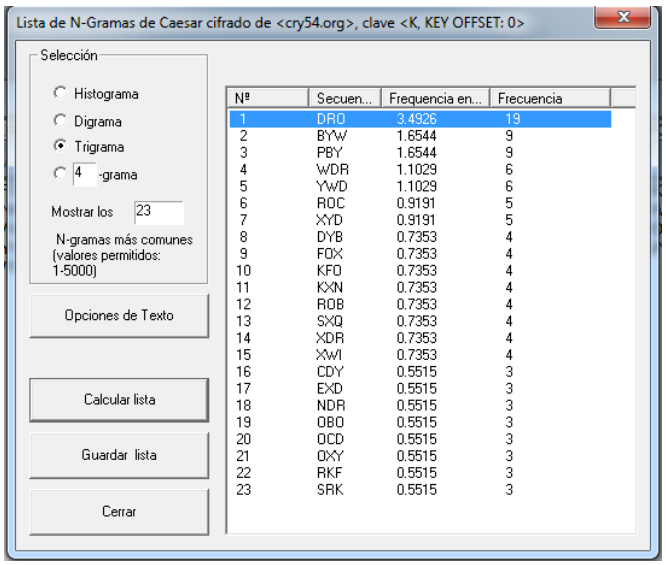
Histograma



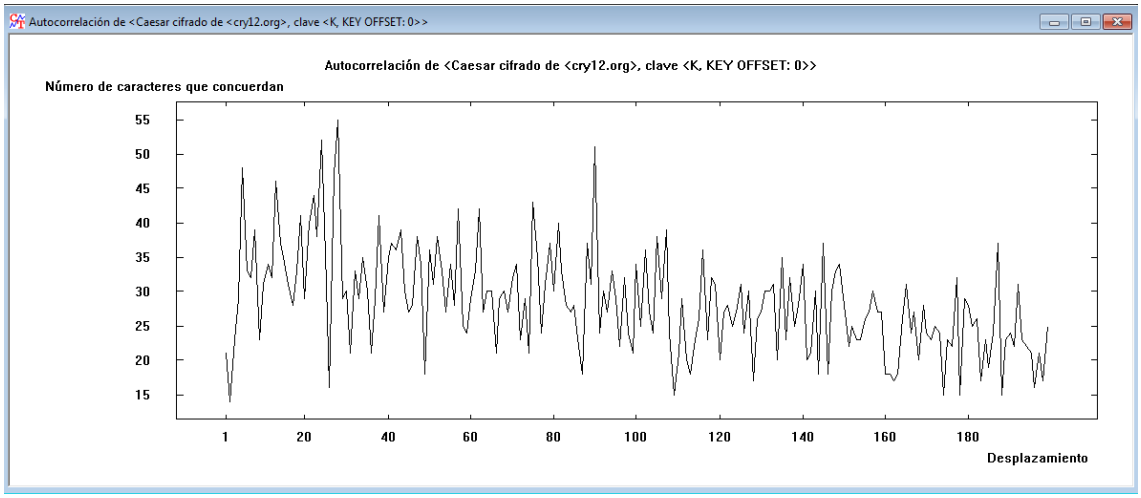
Frecuencia



N-gramas



Autocorrelación:

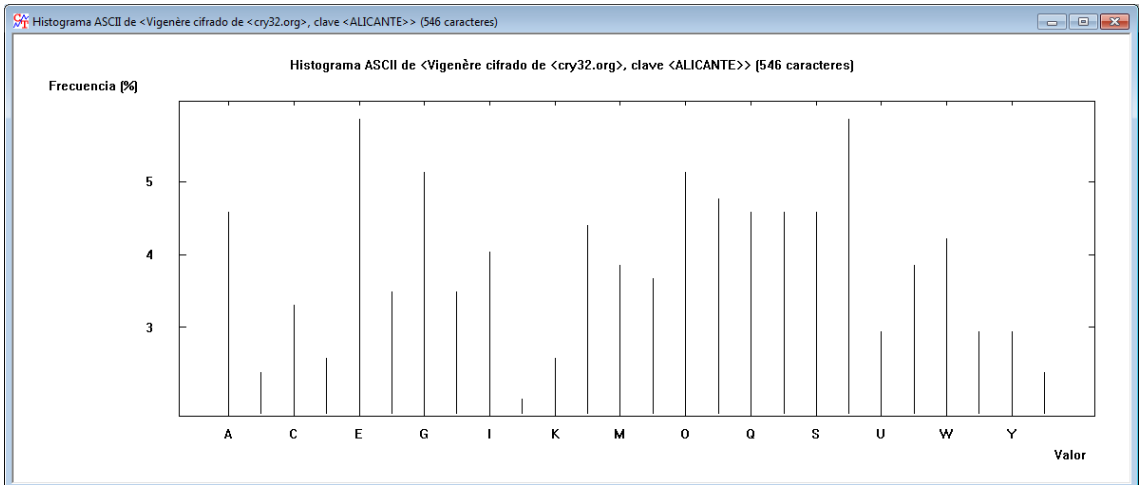


Periocidad: No encontrada. 1.

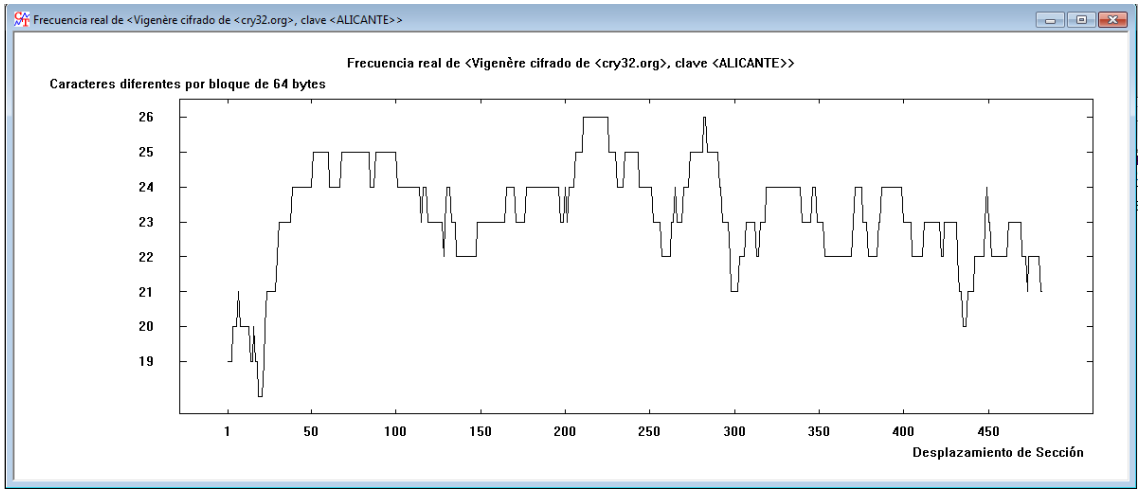
VIGENERE

Entropía: 4.64

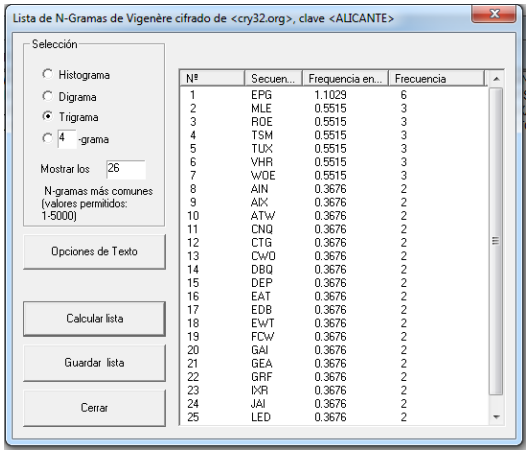
Histograma:



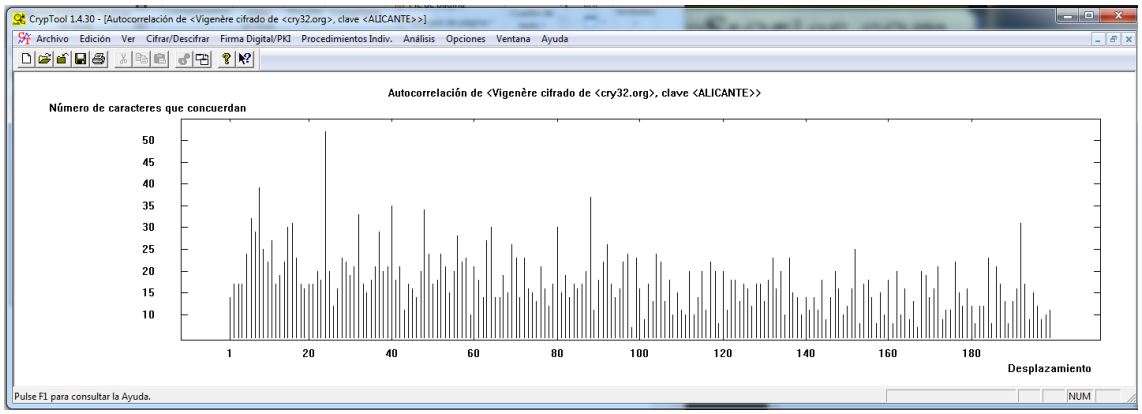
Frecuencia



N-gramas



Correlación



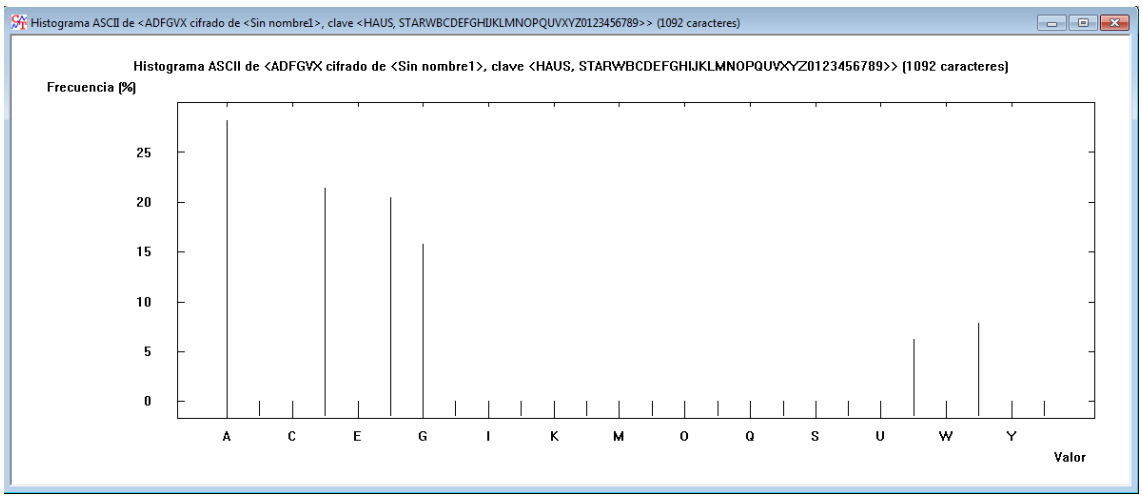
Periodicidad

No encontrada

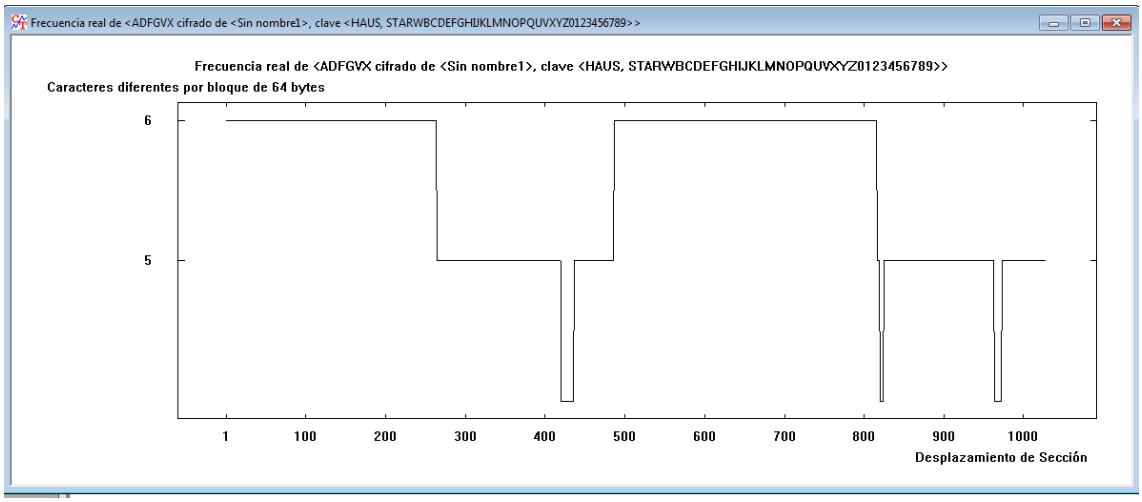
<u>ADFGVX</u>

Entropía: 2.41

Histograma:



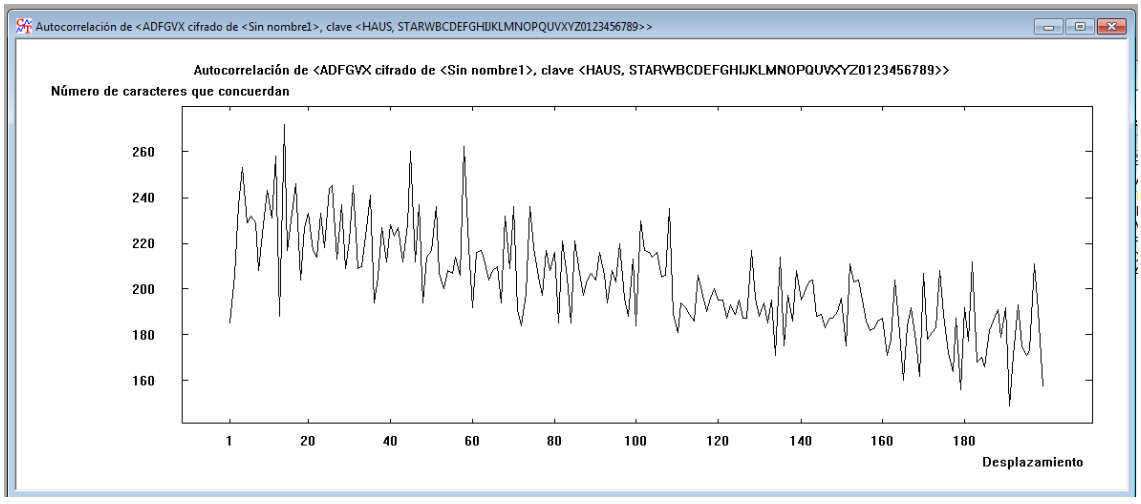
Frecuencias:



N-gramas:

1	AD	7.8827	86
2	AA	7.0577	77
3	DF	6.2328	68
4	FA	6.1412	67
5	AF	5.8662	64
6	FD	5.4995	60

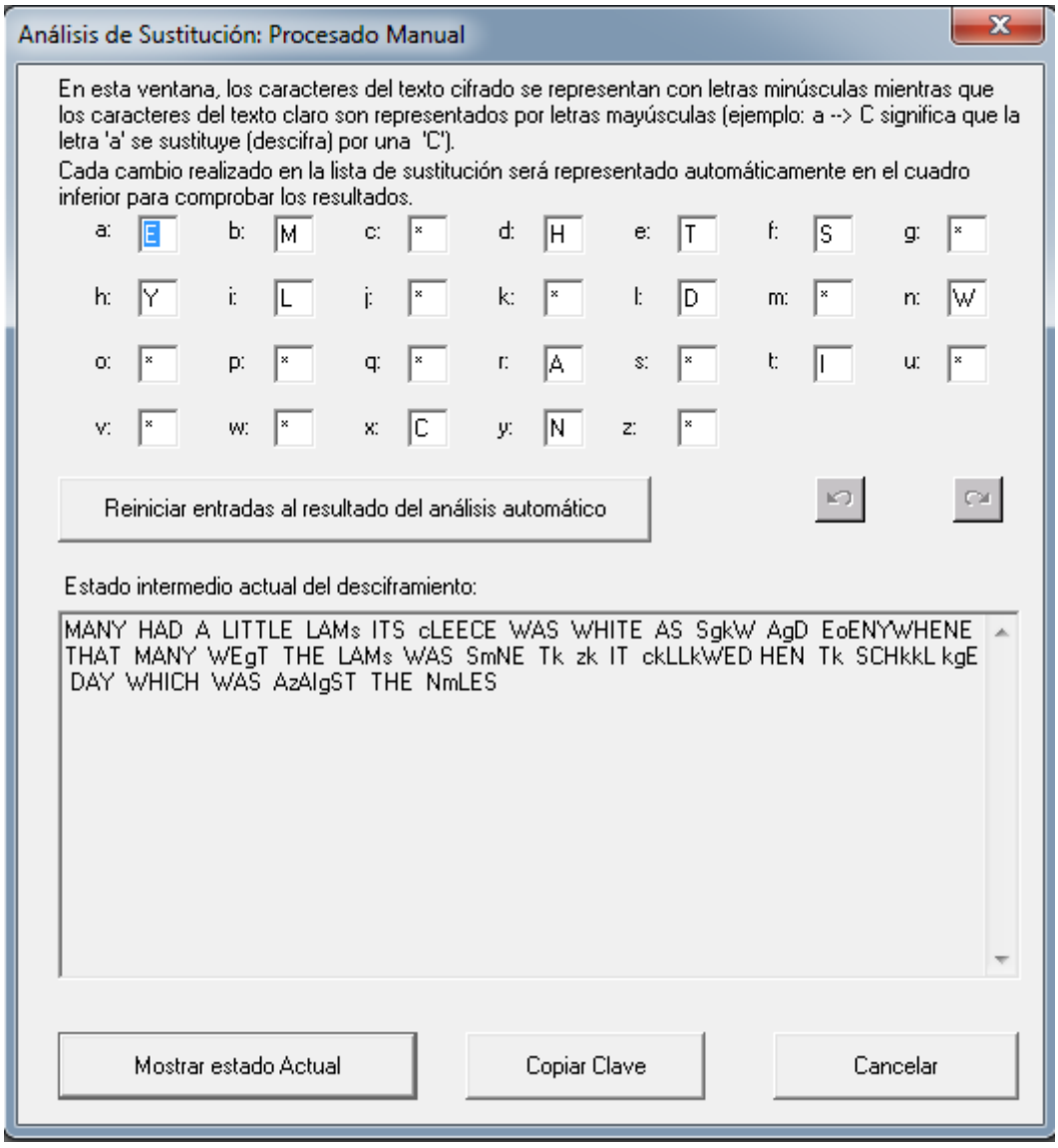
Autocorrelación:



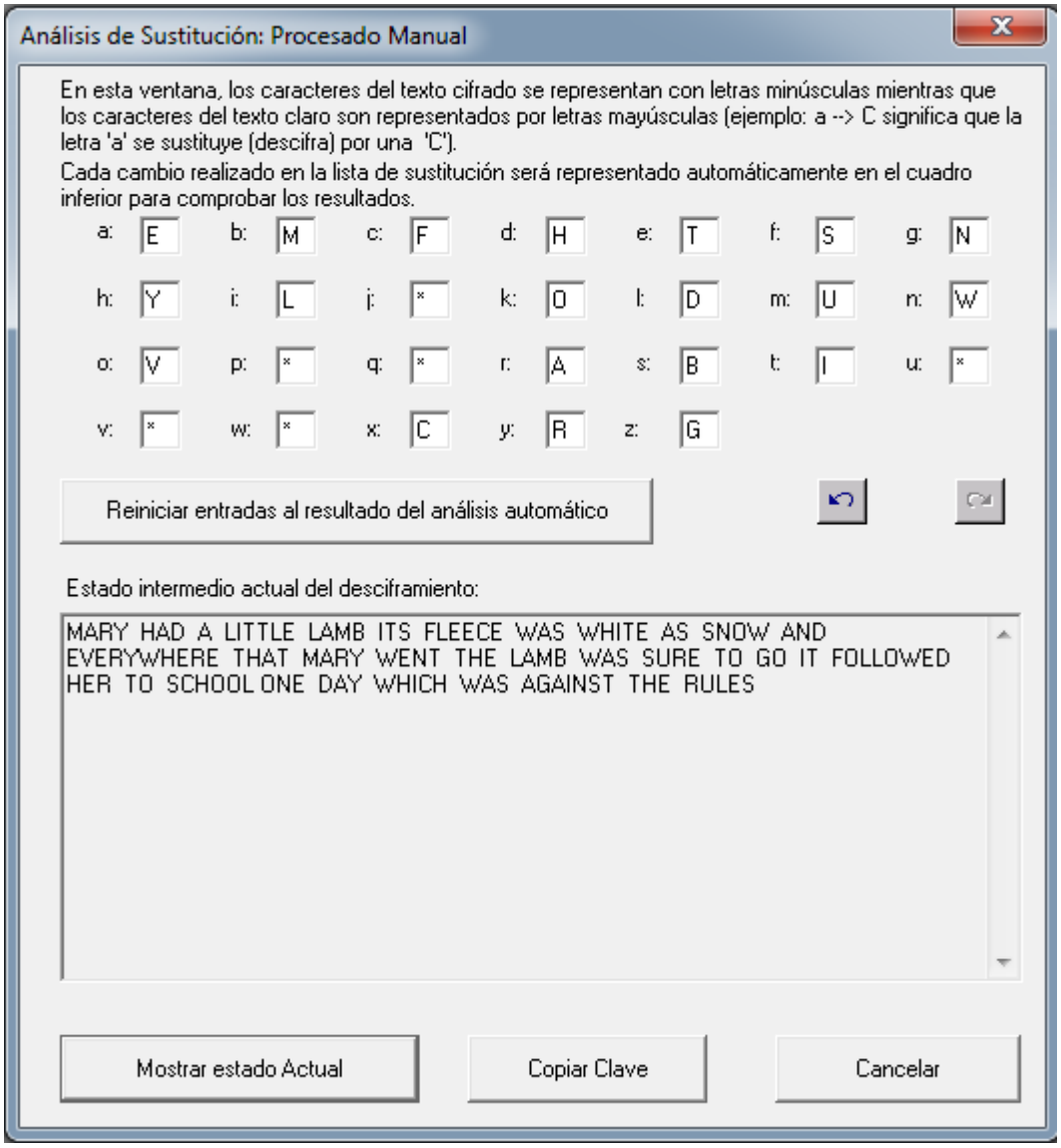
Periocidad: No hay

Ejercicio 7.

Texto monoalfabético. El texto de entrada no sabemos en qué idioma está escrito y por tanto no podemos deducir nada. Lo único que sabemos es que es un algoritmo de cifrado monoalfabético. Probando con la herramienta análisis → cifrado clásico → sustitución y eligiendo la opción de basarse en las palabras más comunes del idioma, podemos ver que resuelve prácticamente el texto.



Ahora buscando lo que queda por descubrir, podemos ver palabras que se pueden intuir fácilmente, Tk es TO y ckllkWED es FOLLOWED, después encontraríamos el resto.



Texto polialfabético.

La herramienta usada para descifrar el texto ha sido el *"análisis vigenere según schroedel"*, usando claves de distintos tamaños basado en palabras del inglés. Para el caso es que tenemos una salida prometedora. La palabra ALIVE descrifra el texto en:

4. Posible Clave:
ALIVE

Texto claro encontrado:
THEAIMEHHSCOMLTHEWHLRUSZAIDTVSPEAROFMAUYTHIUGSOFZHOESHNDSHPPSANKSEALPNGWAEOFCAIBAGEZANDKPNDS
HNDWHYAHESEHISBOPLINGOOTANKWHETOERPFVEWWDICAXQTQ

Aquí se ven palabras claramente del inglés, *THE*.

Aun así no es la solución, pero para encontrarla usamos el método Kasiski, y buscamos trigramas repetidos dentro del texto. Obtenemos {DDP,IYO,LUF,RDD} los cuales se repiten dos veces. Las distancias que separan a cada pareja son {35,26,55,35}. Nos quedamos con 35 ya que está repetido y suponemos que es múltiplo de la distancia. En este punto tendríamos que

probar con claves de tamaño {5,7}. Usando la herramienta "*cifrado de Vigenere"* con el tamaño de 5, nos dice que la palabra puede ser "*ALICE"* y que devuelve

THETIMEHASCOMETHEWALRUSSAIDTOSPEAKOFMANYTHINGSOFSHOESANDSHIPSANDSEALINGWAXOF
CABBAGESANDKINDSHGDWHYTHESEAISBOILINGHOTANDWHETHERPFOEWWDBCAXQMQ

Resultando la solución del texto cifrado.

Ejercicio 9. Texto que venció a Poe.

1) Trigramas

Nº	Secuen...	Frequencia en...	Frecuencia
1	MLW	1.0870	2
2	NBX	1.0870	2
3	NUM	1.0870	2

2) Distancias

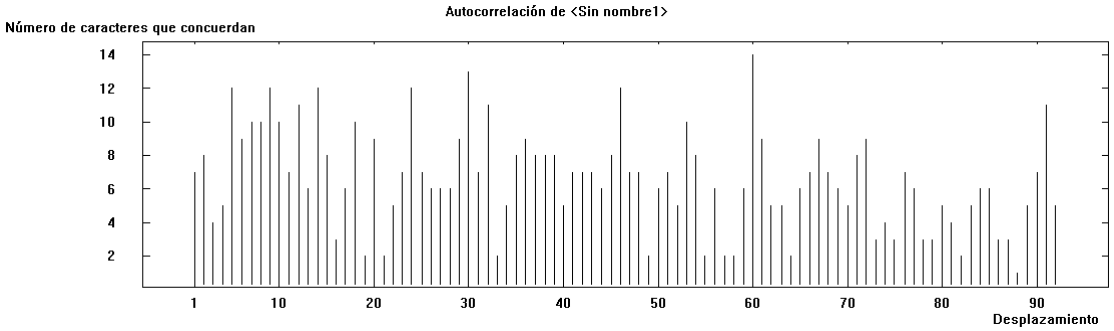
MLW = 91

NBX = 24 =2*2*3

NUM = 72 = 2*2*2*3*3

El periodo debe de ser un divisor de 24 ya que es mcd(24,72) = 24.

3) Autocorrelación



Podemos ver que las secuencia con desplazamiento 60 tiene el máximo número de caracteres iguales que la secuencia original y, por tanto, 60 debe ser un múltiplo de la distancia.
Entonces ahora sabemos que no es 24, si no, un divisor de 12.

4) Análisis de Vigenere.
Para d=12

Que nos devuelve

TWQAXANHECHDWYSITTHETEHTMESSENGIRLRGIVESHERIAETWESACETIQEHIIHTHE
SATYRRANCOURIERENOOIHERSATUDDLOEATERSWHINLVRORDIDGTSTSERATEITIST
UMLXSHRDTHRIEOANSPREVIOYSTSIHEFAULTAIEGNOUORTGETODSBASTYRS

Aquí podemos ver palabras reconocibles

TWQAXANHECHDWYSIT THE TEHT MESSENGIR LRG IVES HERIAETWESACETIQEHIIH THE
SATYRRAN COURIER ENOOIHERSATUDDLOEATERSWHINLVRORDIDGTSTSERATEITIST
UMLXSHRDTHRIEOANS PREVIOYSTSIHE FAULT AIEGNOUORTGETODSBASTYRS

Probamos con MESSENGIR que debe ser MESSENGER y la I aparece en la posición 32 = 8(mod 12). Devolviendo

TW QAXANDECHDW YS IT THAT EHT MESSENGER LRGIVES HERE AE TWE SACE TIME HIIH THE SATURRAN COU RIER ANO OIHER SATUZDLO EATERS WHEN LVRO RDIDG TO TSE RATE IT IS PUMLXSHRD THREE OANS PREVIOUS TS IHE FAULT WIEG NOU OR TGE PODSBASTYRS

Probando a buscar, semejanzas con palabras del inglés, llegamos a

TW QAXANDERHOW YS IT THAT THE MESSENGER ARRIVES HERE AT THE SACE TIME WITH THE SATURGAY COU RIER AND OTHER SATUZDAO PATERS WHEN AVCO RDIDG TO THE CATE IT IS PUBLISHRD THREE DAYS PREVIOUS IS THE FAULT WITG YOU OR TGE POSSMASTYRS

Con la clave NITEDSTATESU, que es UNITEDSTATES habiendo desplazado cíclicamente a la derecha una posición.

Ejercicio 10.

Ahora nos encontramos con un texto, donde no tenemos información. Primero calculamos la entropía y nos dice que se usan todos los caracteres del abecedario. Lo siguiente que hacemos es ver el histograma para ver como de plana es la distribución. Ahora pasamos a buscar n-gramas, y vemos que podemos llegar a encontrar hasta 7-gramas {NUOCZGM, WXIZAYG} que se repiten dos veces. Las distancias son {80,190} que tienen en común los divisores {10,5,2}. Viendo el análisis de correlación podemos ver un patrón cada d=5*i i=1,… por tanto suponemos que la distancia debe de ser 5.

SOUVENTPOURSAMUSERLESHOMMESDEQUIPAGEPRENNENTDESALBATROSVASTESOISEAUXDESMERSQUISUIVENTINDOLENT
SCOMPAGNONSDEVOYAGELENAVIREGLISSANTSURLESGOUFFRESAMERSAPEINELESONTILSDEPOSESSURLESPLANCHESQUE
CESROISDELAZURMALADROITSETHONTEUXLAISSENTPITEUSEMENTLEURSGRANDESAILESBLANCHESCOMMEDESAVIRONSTRAI
NERACOTEDEUXCEVOYAGEURAILECOMMEILESTGAUCHEETVEULELUINAGUERESIBEAUQUILESTCOMIQUEETLAIDLUNAGACESO
NBECAVECUNBRULEGUEULELAUTREMIMEENBOITANTLINFIRMEQUIVOLAITLEPOETEESTSEMBLABLEAUPRINCEDESNUEESQUIH
ANTELATEMPETEETSERITDELARCHERBAUDELAIREEXILESURLESOLAUMILIEUDESHUEESLEMOTPOURETAGEQUATREESTTRAJA
NSESAILESDEGEANTLEMPECHENTDEMARCHER

El texto está en francés usando como clave la palabra SCUBA.

Ejercicio 11.

Tercera palabra = HANKALA. Se ha usado cifrado de cesar con k=3.

Segunda palabra

Tercera palabra = NAVAJO

UT-ZAH! CHA-GEE YIL-TAS SEIS "TSAH WOL-LA-CHEE A-KEH-DI-GLINI TSE-NILL AH-YA-TSINNE NE-AHS-JAH"

it is done! the code is "NAVAJO"

Código sacado de "Navaajo Codetalker Dictionary"

Ejercicio 12.

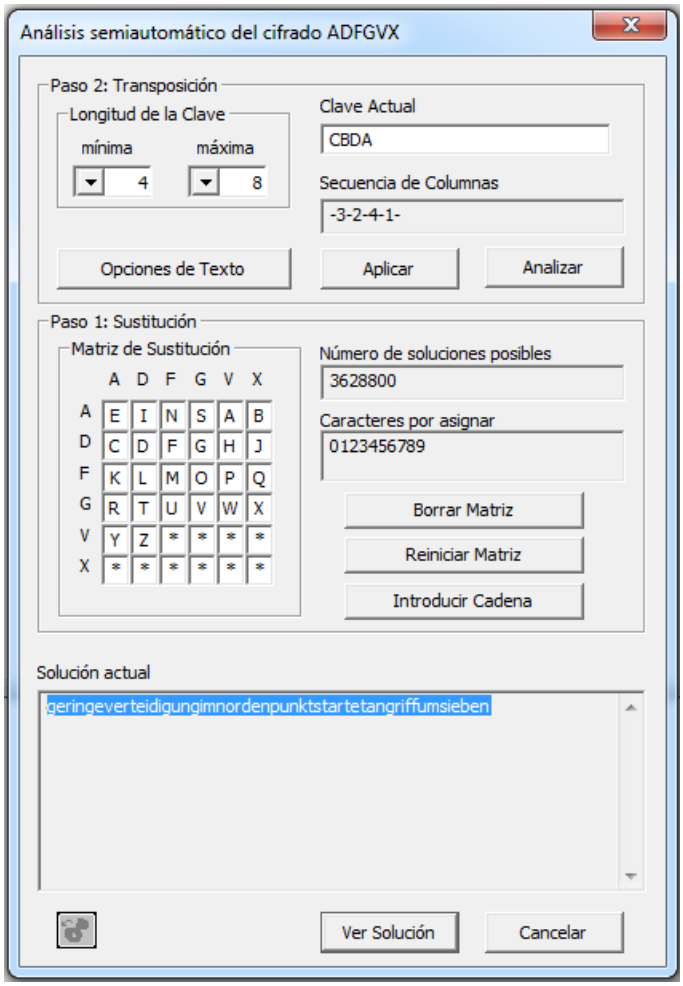
La cabecera da 2 pistas el tamaño de la llave y el tamaño de la llave de trasposición. La trasposición es la que te permite sacar el número de parejas que hay en el texto.

Sabiendo que es de 4 cifras podemos obtener el texto antes de trasponer. La forma de obtener el segundo cifrado es leyendo por columnas y entonces ponemos todo el texto en columnas. Ahora surge la duda de, ¿cuántas filas debe de tener? Muy fácil. Sabemos que tenemos 27 grupos de 4 letras(108 letras) y que deben de ir escritas en 4 columnas, por lo tanto, tenemos que el número de filas es 27. Entonces solo nos queda ir rellenando cada posición. Finalmente el texto queda

AGDA
DAGA
GFAD
GAAG
AAAG
ADGA
DDAD
GDAD
FFGA
DGDA
FFFA
AGFG
ADDA
VFAF
FFGA
DAFG
DGAG
AVAG
ADGA
VDGA
GFAD
DAGA
FFDD
FFGF
DGAA
XAAA
FAAA

Una vez tenemos las columnas, solo falta ordenarlas. Para ello usamos el dato de la distribución, sabiendo que E es la letra más repetida en el texto, seguida de N y después por I. Para encontrar la solución debemos de permutar las columnas 1-2-3-4. En total hay 24 posibilidades, y a cada posibilidad hay que buscar las parejas más repetidas, para tratar de encontrar una configuración que resuelva el problema. También es crucial el dato del tamaño de la clave de sustitución ya que permite saber si las posibles soluciones se deben de descartar sin hacer la prueba, únicamente comprobando la factibilidad de la posición de las letras E,N,I dentro de la matriz de sustitución.

Probando, encontramos



Texto plano: geringe verteidigung im norden punkt startet angriff um sieben