Seguridad de los Sistemas Informáticos

Práctica 1: Criptografía

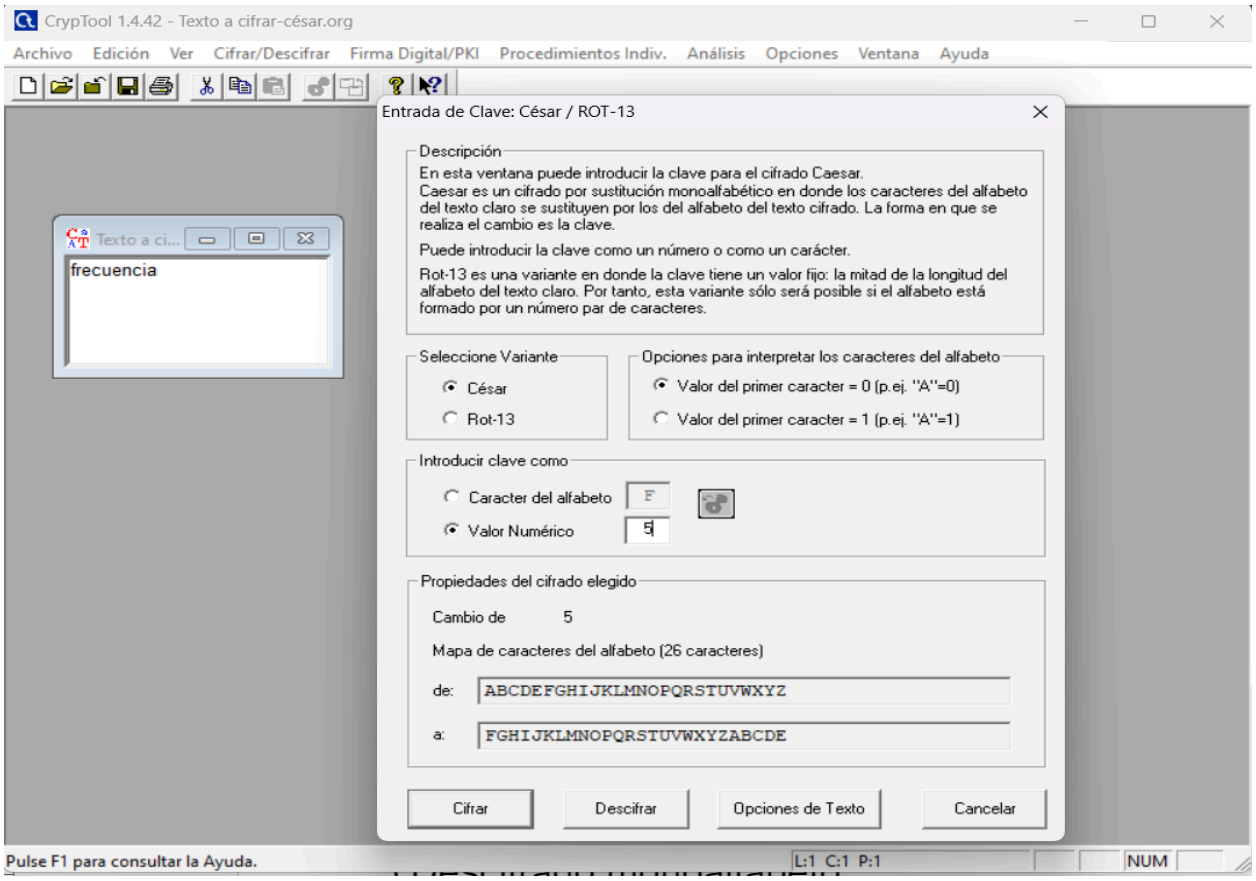
Grupo 3.1

1. Uso Básico de CrypTool

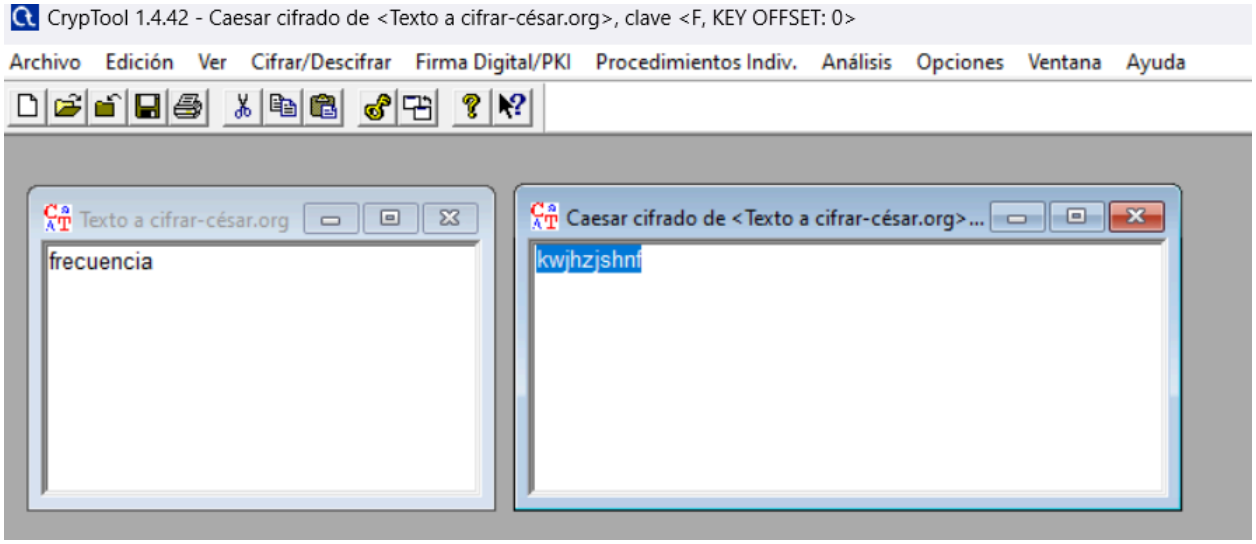
1.1. Realicen pruebas de cifrado y descifrado con los algoritmos vistos en clase de teoría

Cifrado Cesar

Para este ejemplo tomaremos el texto “frecuencia” al que aplicaremos un desplazamiento 5.

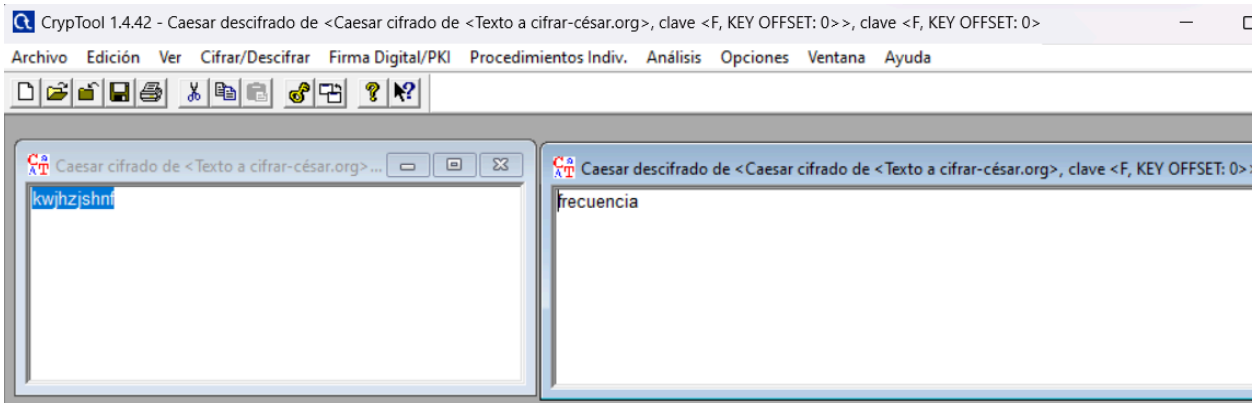


Dando como resultado : kwjhzjshnf

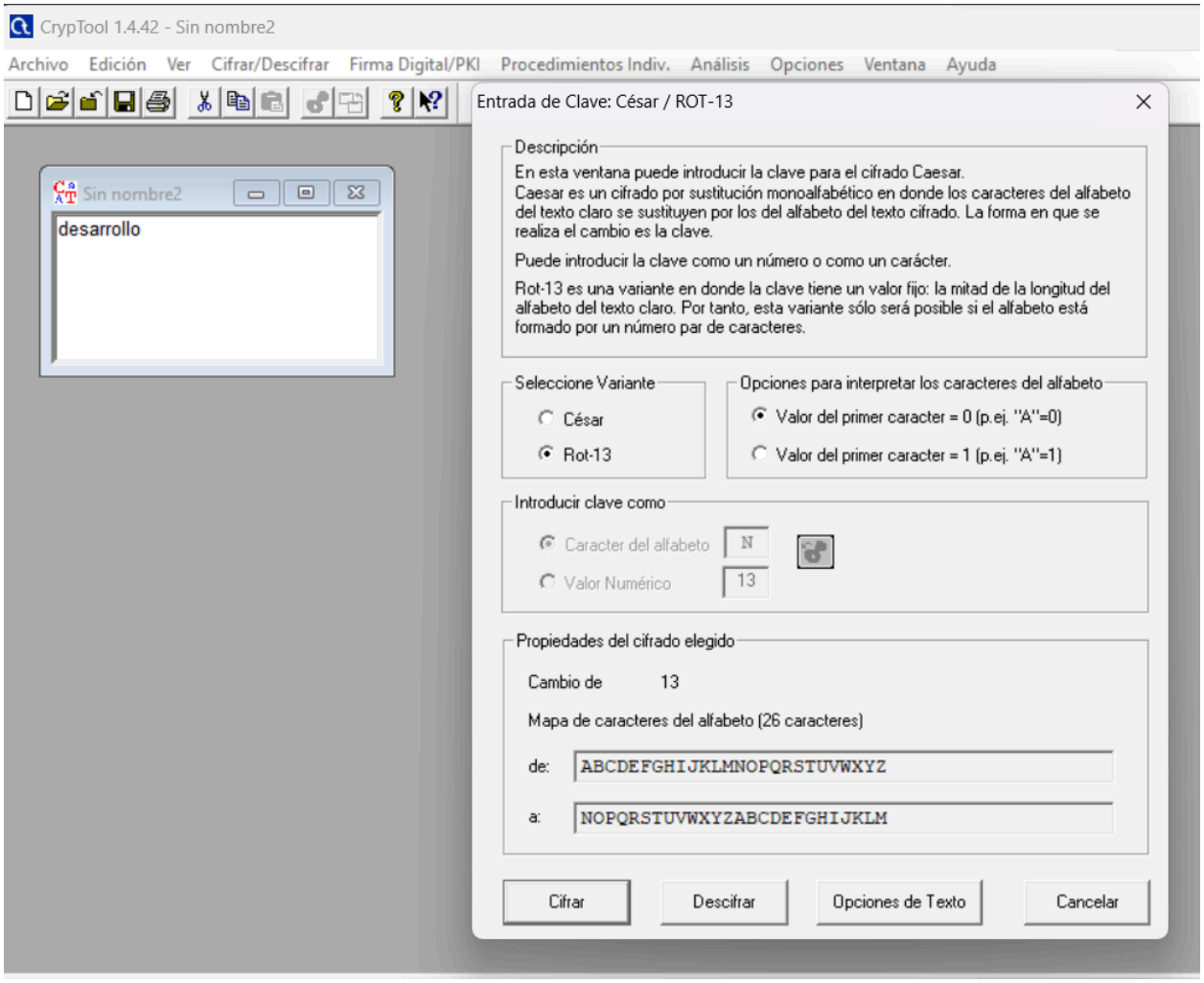


Para el Descifrado

Igual aplicamos un desplazamiento 5, quedando así:

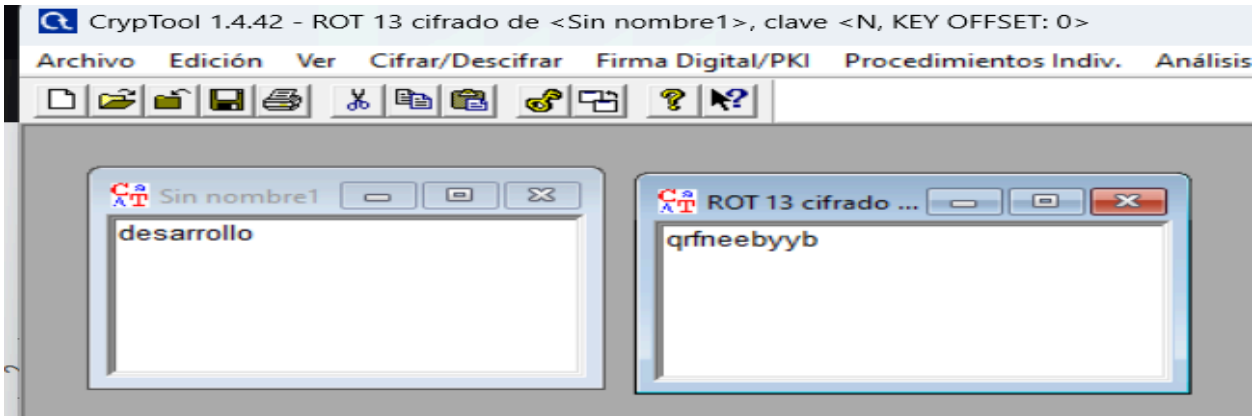


Rot / 13

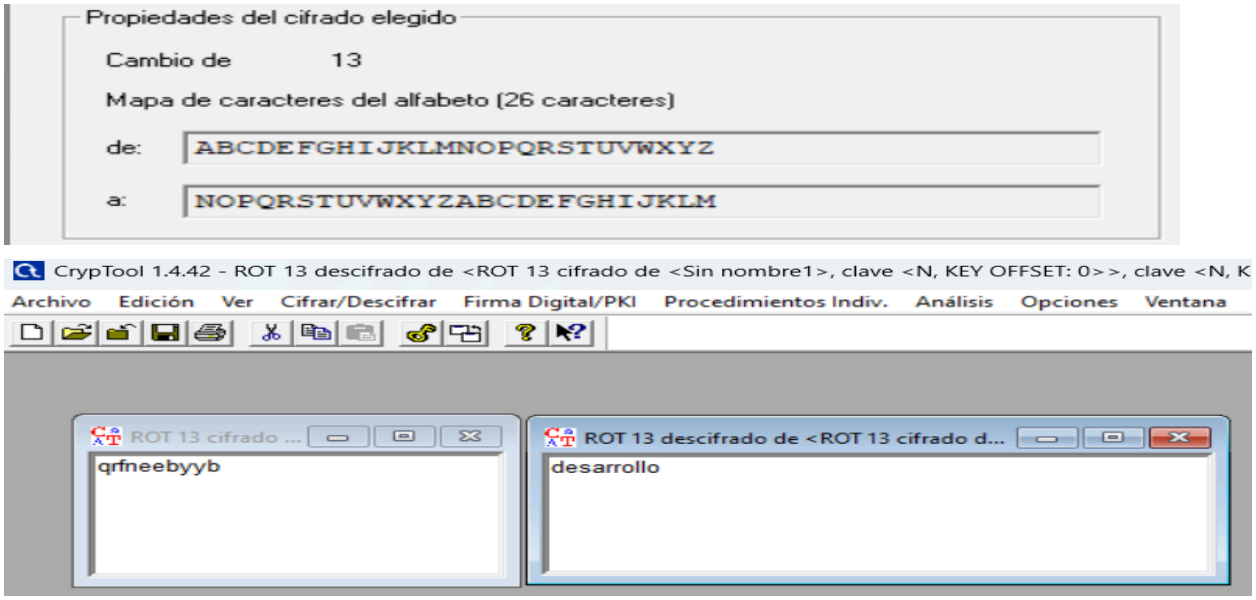


Este cifrado lo que hace es tomar el alfabeto que está conformado por un número par de 26 caracteres y lo divide en dos , quedando un desplazamiento 13.

El texto introducido quedaría cifrado de la siguiente manera:

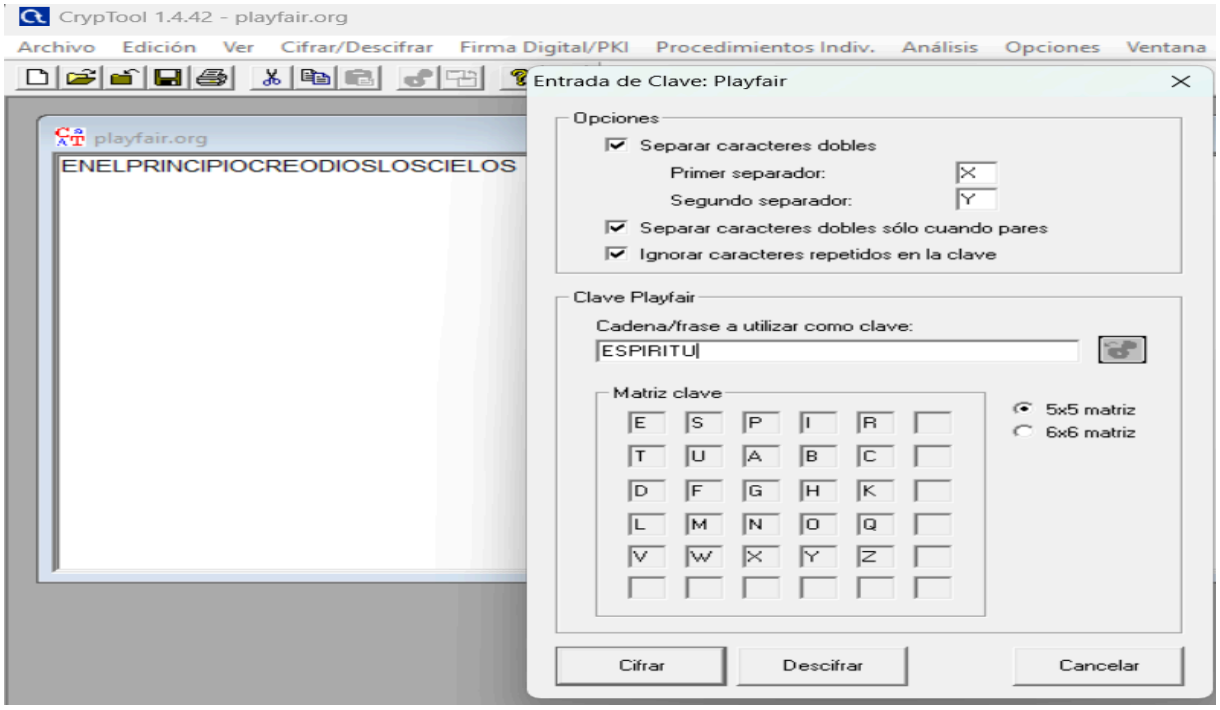


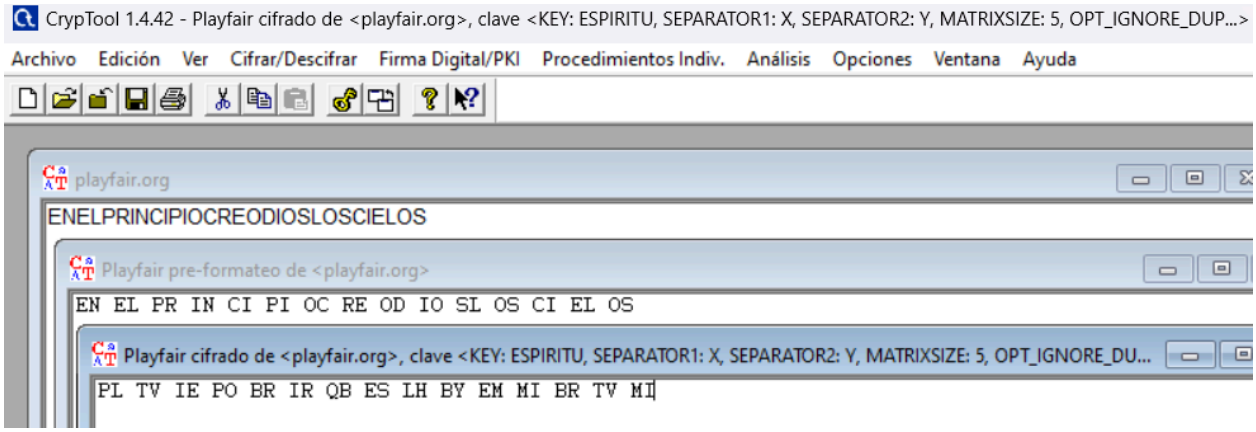
Descifrado
Aplicamos el desplazamiento 13 y procedemos a la sustitución de los caracteres del alfabeto



Playfair

La matriz se construye insertando una clave (en el ejemplo: ESPIRITU y se completa con el resto de letras del abecedario, excluyendo las de la clave. Utilizando una matriz 5x5

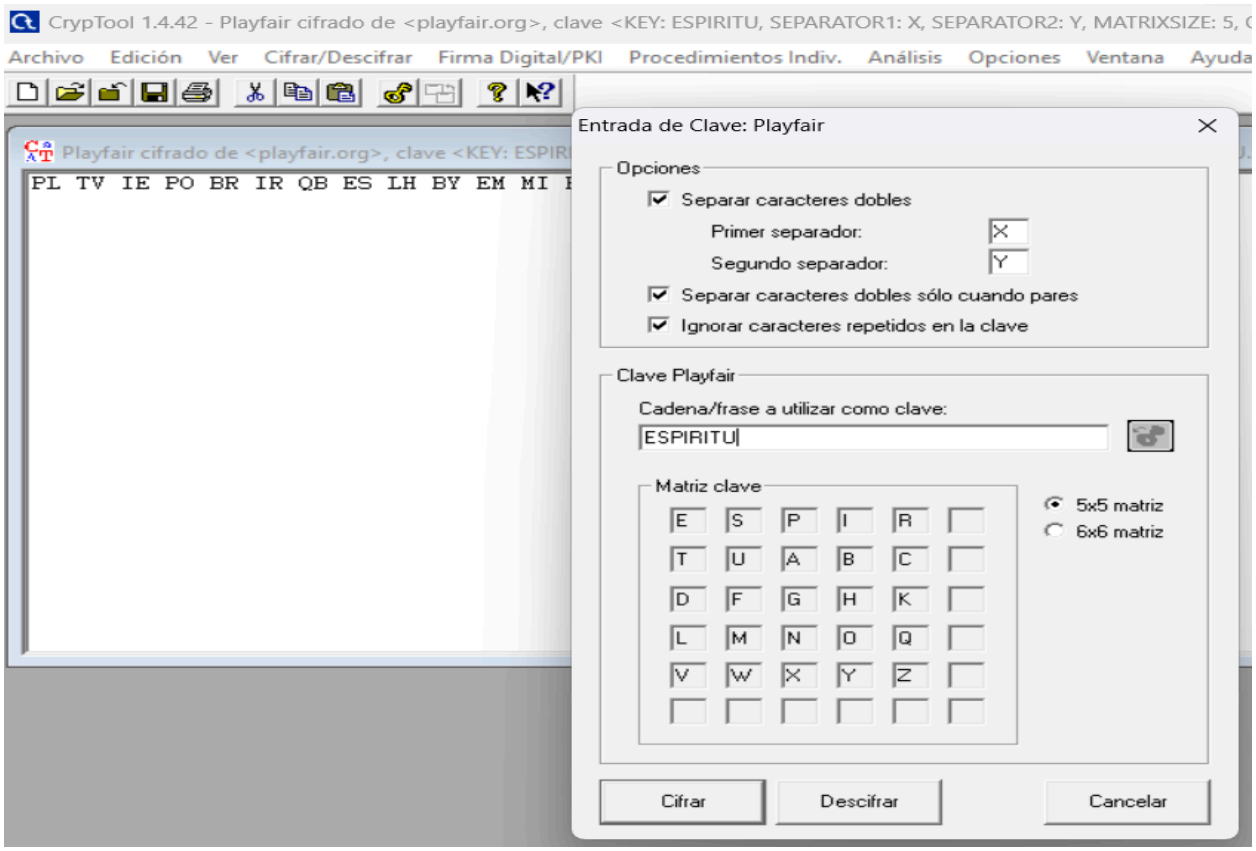


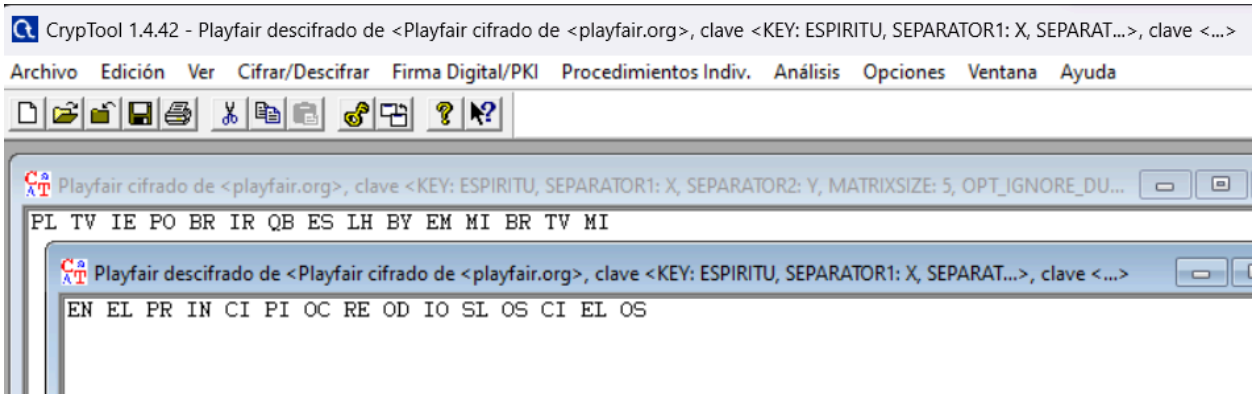


Dando el texto cifrado: **PL TV IE PO BR IR QB ES LH BY EM MI BR TV MI**

Descifrado:

Tomamos el texto cifrado y se introduce la misma clave: ESPIRITU





Texto: **EN EL PR IN CI PI OC RE OD IO SL OS CI EL OS**
ENELPRINCIPIOCREODIOSLOSCIELOS

1.2. Opciones de Cryptool para el criptoanálisis de algoritmos de sustitución monoalfabeto.

Cryptool utiliza dos métodos para el criptoanálisis de algoritmos de sustitución monoalfabeto:

Método 1 basado en el análisis de frecuencia de pares de caracteres en el texto.
Este método analiza la frecuencia de los caracteres en el texto cifrado y determina la clave basándose en una distribución estándar de pares de caracteres.
Los mejores resultados obtenidos por este método se consiguen con textos largos.
Está incluido el reconocimiento de idioma del mensaje y se permite analizar textos de los que se haya eliminado el carácter del espacio.

Fuente: Thomas Jakobsen "A Fast Method for Cryptanalysis of Substitution Ciphers", Cryptologia 19:3, 1995

El artículo de 1995 de Thomas Jakobsen, A Fast Method for Cryptanalysis of Substitution Ciphers, presenta un algoritmo que refina las suposiciones iniciales de la clave mediante pasos iterativos. El método aprovecha el análisis de frecuencia de diagramas, centrándose en los patrones estadísticos de pares de letras en el texto cifrado y comparándolos con distribuciones típicas de diagramas en el lenguaje de texto simple. Este enfoque minimiza la necesidad de descifrar completamente en cada paso, lo que acelera el proceso. El algoritmo de Jakobsen es eficiente tanto para cifrados de sustitución monoalfabéticos como polialfabéticos.

Método 2 basado en el reconocimiento de las palabras más frecuentes de un idioma.
Este método está basado en una lista de palabras más frecuentes de una lengua en particular. Las palabras del texto cifrado son comparadas (de acuerdo a este patrón) con las palabras de la lista.
Usando un árbol de búsqueda, se determina la sustitución que es compatible con un mayor número de las sustituciones parciales encontradas. Este método puede procesar textos en Alemán e Inglés en los que se haya respetado el carácter del espacio.

Fuente: George W. Hart " To Decode Short Cryptograms", Communications of the ACM, Sep 1994, Vol 37, No.4

El artículo "To Decode Short Cryptograms" (Cómo descifrar criptogramas breves) de George W. Hart, publicado en la edición de septiembre de 1994 de Communications of the ACM, se centra en las técnicas para resolver criptogramas (breves rompecabezas en los que se cifra una frase o cita mediante un cifrado de sustitución). Estos rompecabezas son populares entre los entusiastas de los juegos de palabras recreativos y aparecen con frecuencia en los periódicos.

El trabajo de Hart destaca cómo el análisis de frecuencias y los patrones en el idioma inglés pueden simplificar la resolución de los cifrados de sustitución, incluso para textos más breves. Explora estrategias prácticas de descifrado, destacando que reconocer patrones de palabras comunes o letras de alta frecuencia (como "E" o "T") puede proporcionar pistas cruciales. Además, el artículo profundiza en la idea de reconstruir el texto simple mediante el análisis de las permutaciones utilizadas en el mensaje cifrado, lo que ofrece información sobre cómo se pueden revertir las reglas de cifrado.

3 Algoritmo cifrado simétrico monoalfabeto

3.1 Explicación algoritmo

Es un cifrado simétrico de sustitución monoalfabético en el que la clave es una palabra o conjunto de carácter iniciales que desplazan el resto de caracteres.

Ejemplo de cifrado:

```
$ python monoalfabeto.py
Enter 'e' for encryption or 'd' for decryption (q to quit) or 'help' for help: e
Enter the key: ALFA
Key set to: ALFA
Enter the plaintext (uppercase, no spaces): TEXTODEPRUEBAPARALAMEMORIAAENTREGAR
Encrypted text: RHYSKHIMSQHLCKLQLFLKMRMTDCLDOSWMDFSW
```

Ejemplo de descifrado:

```
$ python monoalfabeto.py
Enter 'e' for encryption or 'd' for decryption (q to quit) or 'help' for help: d
Enter the key: ALFA
Key set to: ALFA
Enter the ciphertext (uppercase): RHYSKHIMSQHLCKLQLFLKMRMTDCLDOSWMDFSW
Decrypted text: TEXTODEPRUEBAPARALAMEMORIAAENTREGARX
```

3.2 Salida -help

Playfair Cipher Program

This program allows you to encrypt and decrypt messages using the Playfair cipher.

Parameters:
- Enter '-e' to encrypt a message with file input.
- Enter '-d' to decrypt a message with file input.
- Enter '-E' to encrypt a message with args input.
- Enter '-D' to decrypt a message with args input.
- Enter '--key' specify a key to use.

Commands interactive mode:
- Enter 'e' to encrypt a message.
- Enter 'd' to decrypt a message.
- Enter 'q' to quit the program.

Encryption Process:
1. Input your plaintext (uppercase letters only, no spaces).
2. The program will encrypt your message using the specified key.
3. If there are duplicate letters in a pair, an 'X' will be added.
4. The output will be your encrypted text.
5. (Optional file mode) The encrypted text will be saved to a file named 'enc-out-N.txt', where N is an auto-incrementing number.

Decryption Process:
1. Input your ciphertext (uppercase letters only).
2. The program will decrypt your message using the same key used for encryption.
3. The output will be your decrypted text.
4. (Optional file mode) The decrypted text will be saved to a file named 'dec-out-N.txt', where N is an auto-incrementing number.

Note:

- The key should consist of uppercase letters and will be used to create a Playfair matrix.
- Each encryption or decryption operation will create a new output file with an incremented number.
- The counter for file naming is stored in a local 'counter.json' file.

Example Key: "MONAR"

Enjoy using the Playfair cipher!

3.3 Comando cifrado y descifrado

python3 monoalfabeto.py -e ./out-deliver/texto1.txt
python3 monoalfabeto.py -e ./out-deliver/texto2.txt

4. Algoritmo vigenère

4.1 Funcionamiento e implementación

El algoritmo de cifrado explicado por carácter primero calcula el desplazamiento y luego suma su valor al del carácter a cifrar rotando el desplazamiento entre los caracteres de la clave.

En la implementación se calcula el ordinal del carácter correspondiente en la clave y se resta con respecto al ordinal de la A para obtener el desplazamiento. Posteriormente se calcula el ordinal del carácter a cifrar, se suma el desplazamiento, se calcula el módulo tamaño del alfabeto y se le suma el ordinal de A para obtener el carácter cifrado.

4.1 Salida -help

Enter 'e' for encryption or 'd' for decryption (q to quit) or 'help' for help: help

Vigenère Cipher Program

This program allows you to encrypt and decrypt messages using the Vigenère cipher.

Parameters:
- Enter '-e' to encrypt a message with file input.
- Enter '-d' to decrypt a message with file input.
- Enter '-E' to encrypt a message with args input.
- Enter '-D' to decrypt a message with args input.

- Enter '--key' specify a key to use.

Commands interactive mode:

- Enter 'e' to encrypt a message.
- Enter 'd' to decrypt a message.
- Enter 'q' to quit the program.

Encryption Process:

1. Input your plaintext (uppercase letters only).
2. The program will encrypt your message using the specified key.
3. The output will be your encrypted text.
4. (Optional file mode)The encrypted text will be saved to a file named 'enc-out-N.txt', where N is an auto-incrementing number.

Decryption Process:

1. Input your ciphertext (uppercase letters only).
2. The program will decrypt your message using the same key used for encryption.
3. The output will be your decrypted text.
4. (Optional file mode)The decrypted text will be saved to a file named 'dec-out-N.txt', where N is an auto-incrementing number.

Note:

- The key should consist of uppercase letters.
- Each encryption or decryption operation will create a new output file with an incremented number.
- The counter for file naming is stored in a local 'counter.json' file.

Enjoy using the Vigenère cipher!

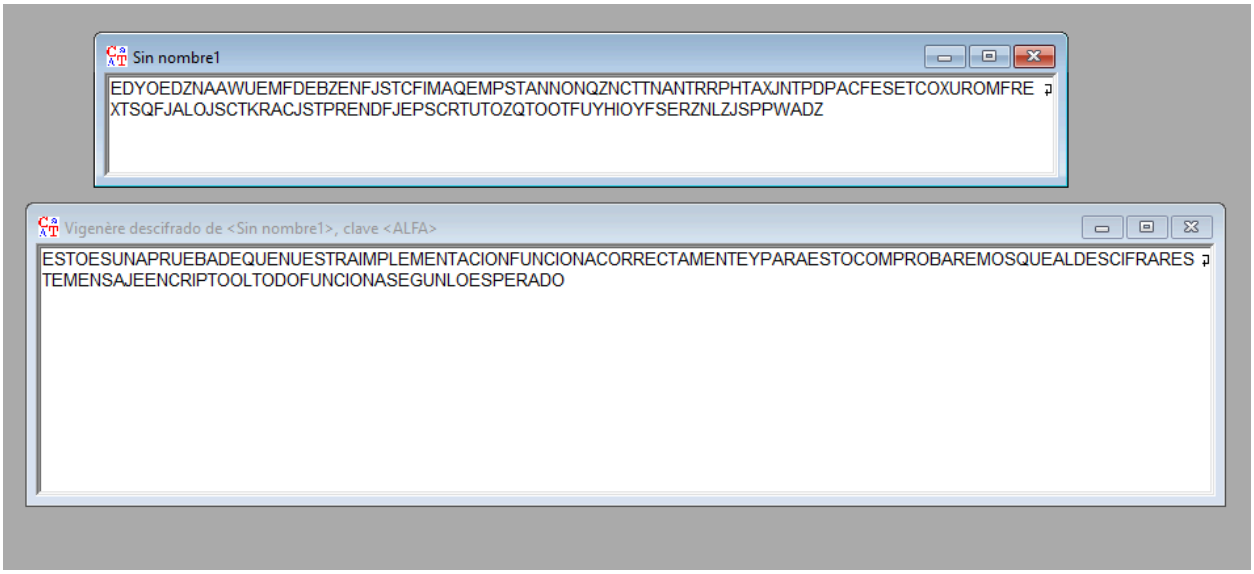
4.3 Evidencias correcta implementación

Para mostrar que nuestro algoritmo funciona correctamente vamos a cifrar un simple mensaje y después analizarlo en cryptool v1. Con esto debemos obtener el mensaje original y la clave.

En la siguiente imagen vemos cómo utilizamos nuestra implementación para cifrar:

```
$ python vigenere.py
Enter 'e' for encryption or 'd' for decryption (q to quit) or 'help' for help: e
Enter the key: ALFA
Key set to: ALFA
Enter the plaintext (uppercase): ESTOESUNAPRUEBADEQUENUESTRAIMPLEMENTACIONFUNCIONACORRECTAMENTEYPARAESTO
COMPROBAREMOSQUEALDESCIFRARESTEMENSAJEENCRIPTOOLTODOFUNCIONASEGUNLOESPERADO
Encrypted text: EDYOEDZNAAWUEMFDEBZENFJSTCFIMAQEMPSTANNONQZNCTTNANTRRPHTAXJNTPDPACFESETCOXUROMFREXTSQFJA
LOJSCTKRACJSTPRENDFJEPSCRTUTOZQTOOTFUYHIOYFSERZNLZJSPPWADZ
```

Y según cryptool el resultado es:



Por lo que se demuestra que nuestra implementación de Vigenère funciona según lo esperado.

4.4 Comando cifrado y descifrado

python3 monoalfabeto.py -e ./out-deliver/texto3.txt

5. Descifrado monoalfabeto

5.1. Descifrado 1

Fragmento descifrado: 1.4_fragmento1_cif.txt

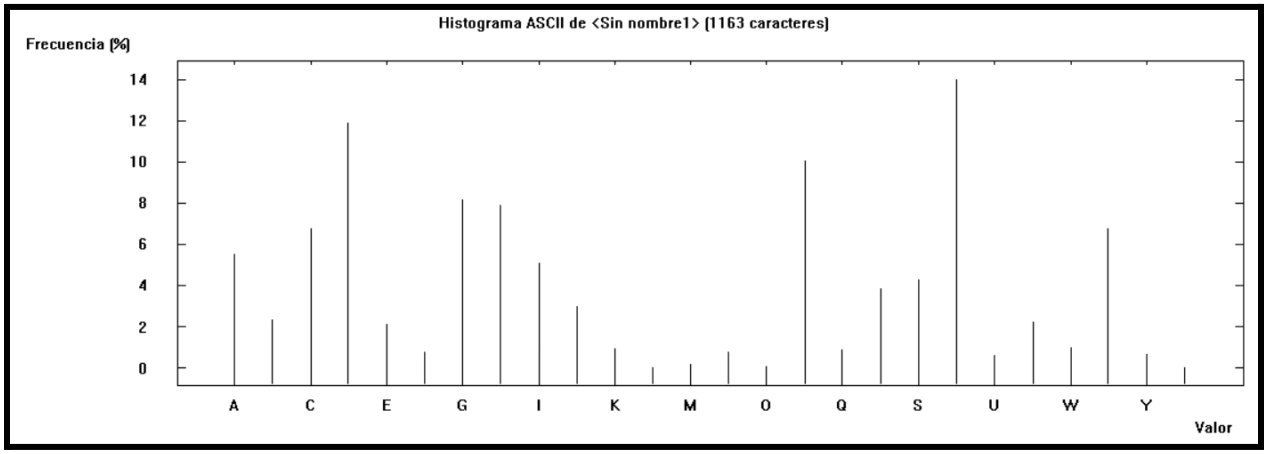
Texto descifrado:

LASHISTORIASDELOSVIAJESDERETORNODELOSGRIEGOSSERECOGIERONENUNREL
ATOEPICOESPECIALDENTRODELCICLOTROYANONOSTOIOLOSREGRESOSUNODESU
STEMASCENTRALESFUELAIRADEATENEAPROVOCADAPORUNACTODESACRILEGIOC
OMETIDOENSUSANTUARIOPORAYAXELMENORDURANTEELSAQUEODETROYAQUEFU
EDIRIGIDANOSOLOCONTRAELSINOTAMBIENCONTRALOSGRIEGOSENGENERALPORH
ABERFRACASADOALCASTIGARLOLADIOSASEMBROLADISCORDIAENELCAMPOGRIEG
OEHIZOQUEAGAMENONYMENELAODISCUTIERANPORLOQUEVOLVIERONACASAPOR
SEPARADOACOMPANADOSDEDISTINTASSECCIONESDELEJERCITOELLAENVIOENTO
NCESUNATERRIBLETORMENTACONTRALAFLOTADEAGAMENONALGUNOSHEROESPE
RDIERONELRUMBOOTROSMURIERONMIENTRASQUEUNOSPOCOSEVITARONTODOSL
OSPELIGROSDELMARALHABERVIAJADOPORTIERRALOSDIFERENTESITINERARIOSYD
ESTINOSDELOSGRIEGOSQUERETORNABANFORMARANELTEMADELAPRIMERAMITAD
DELPRESENTECAPITULOENPARTICULARSONCUATROLOSHEROESQUETIENENHISTO

RIASINTERESANTESASOCIADASCONSUSREGRESOSODISEOVAGOPORTIERRASLEJA
NASYLLEGOAREINOSEXTRANOSYMARESDISTANTESTALCOMOSERECOGEENELSEG
UNDORELATOEPICODEHOMEROMIENTRASQUENEOPTOLEMOHIJODELFALLECIDOAQ
UILESVIAJOPORTIERRASIGUIENDOELCONSEJODESUDIVINAABUELAYSEESTABLECIO
ENEPIROENLOSMARGENESNOROCCIDENTALESDEGRECIACONLAVIUDADEHECTORC
OMOSUCONCUBINAYLAHIJADEHELENACOMOESPOSA

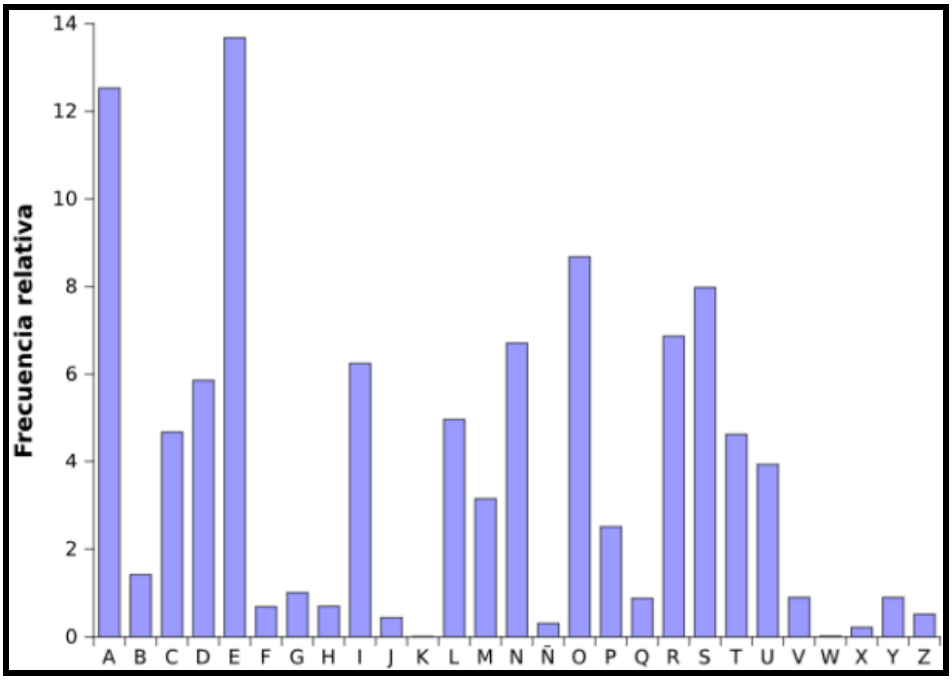
Tipo de cifrado: César
Desplazamiento: 15

Procedimiento de descifrado:
Realizando un análisis de frecuencias con CrypTool hemos podido llegar a las siguientes conclusiones:



En el texto cifrado las letras más comunes, por este orden, son la T, la D, la P, la G y la H.

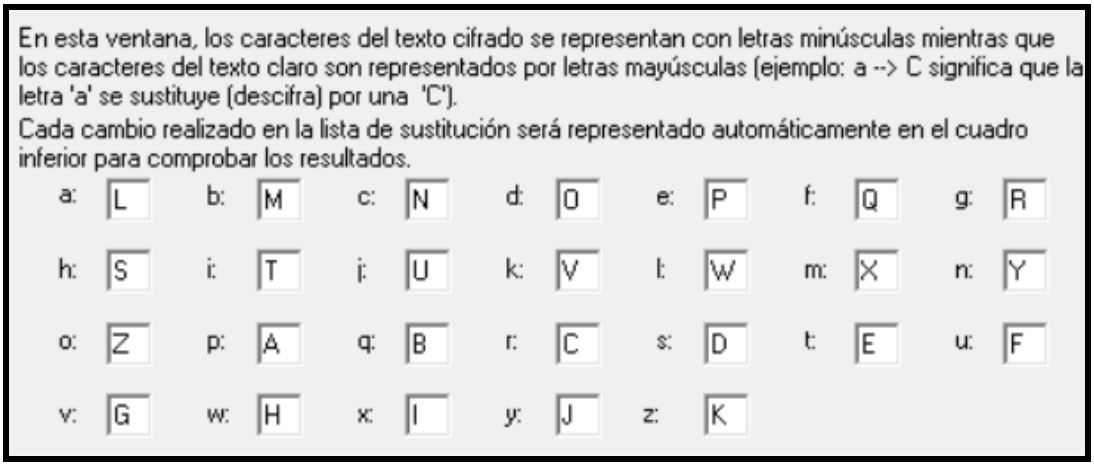
Sabiendo esto, hemos utilizado el gráfico de los apuntes de análisis de frecuencias de la parte teórica de la asignatura.



A partir de ambos gráficos comenzamos a hacer deducciones:

1. T (cifrada) -> E (descifrada) [distancia de 15 caracteres.]
2. D (cifrada) -> O (descifrada) [distancia de 15 caracteres.]
3. P (cifrada) -> A (descifrada) [distancia de 15 caracteres.]

En este caso la frecuencia de aparición de A y O están invertidas, nos dimos cuenta porque si no las distancias no eran iguales, y en nuestra metodología siempre analizamos primero buscando el cifrado César.
En cuanto hemos visto tres distancias iguales, (objetivamente ya con 2 es sospechoso de ser cesar) simplemente hemos pasado al descifrado por procesado manual en CrypTool.



Posible algoritmica de cifrado (pseudocódigo):

Teniendo en cuenta que los mas normal al cifrador es escoger la clave de cifrado a la hora de cifrar y no hacer una clave fija en el codigo, este ha sido el resultado del posible algoritmo de cifrado.

```
ALGORITMO CifradoCesar
   ENTRADA: texto_claro (cadena de texto), clave (entero)
   SALIDA: texto_cifrado (cadena de texto)

   INICIO
      texto_cifrado ← ""  // Cadena vacía para almacenar el resultado
      desplazamiento ← clave MOD 25  // Asegurarse de que el desplazamiento esté
dentro del rango [0-24]

      PARA cada caracter en texto_claro HACER
            nueva_letra ← (ASCII(caracter) - ASCII('A') + desplazamiento) MOD 25 +
ASCII('A')
            texto_cifrado ← texto_cifrado + nueva_letra
            CONTINUAR
      FIN PARA

      RETORNAR texto_cifrado
   FIN
```

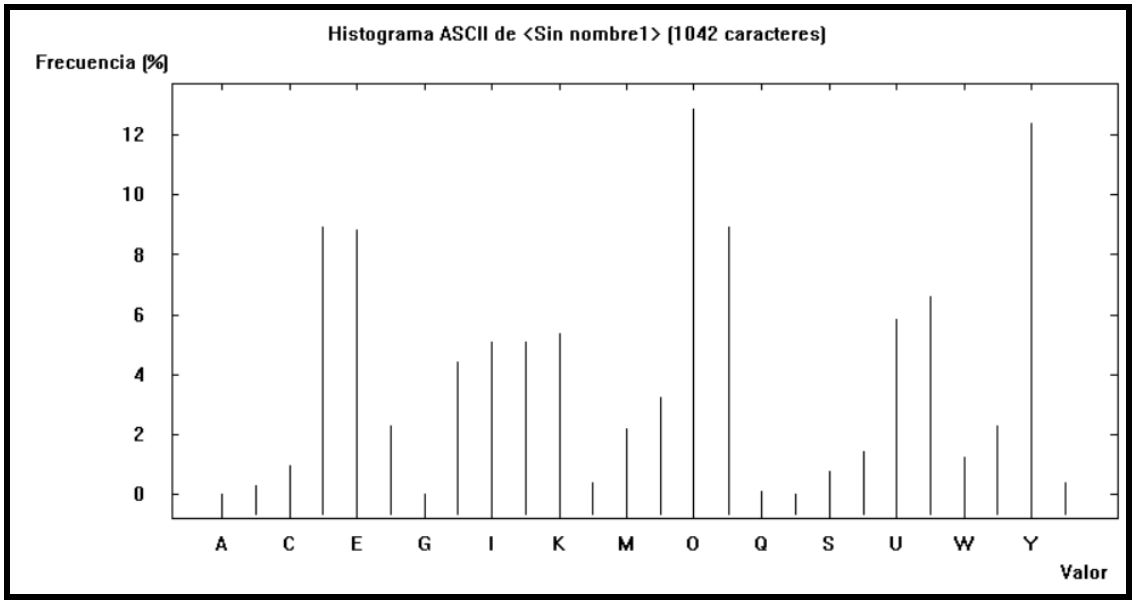
5.2. Descifrado 2

Fragmento descifrado: 2.1_fragmento1_cif.txt
Texto descifrado:

CONESEMIRARVAGOYDISTRAIDOQUEESENLOSMOMENTOSDEINTENSAAMARGURAC
OMOUNGIROANGUSTIOSODELALMASOBRESIMISMAVEIAPASARPORUNAYOTRABAND
ADELJARDINGENTESPRESUROSASOINDOLENTESUNOSLLEVABANUNDUROOTROSIB
ANABUSCARLOPASABANCOBRADORESDELBANCOCONELTALEGUILLOALHOMBROCA
RRICOCHESCONBOTELLASDECERVEZAYGASEOSACARROSFUNEBRESENELCUALER
ACONDUCIDOALCEMENTERIOALGUNOAQUIENNADAIMPORTABANYALOSDUROSENLA
STIENDASENTRABANCOMPRADORESQUESALIANCONPAQUETESMENDIGOSHARAPO
SOSIMPORTUNABANALOSSENORESCONRAPIDAVISIONBENINAPASOREVISTALOSCAJ
ONESDETANTATIENDAALOSDISTINTOSCUARTOSDETODASLASCASASALOSBOLSILLO
SDETODOSTRANSEUNTESBIENVESTIDOSADQUIRIENDOLACERTIDUMBREDEQUEEN
NINGUNODEAQUELLOSREPLIEGUESDELAVIDAFALTABAUNDURODESPUESPENSOQU
ESERIAUNPASOMUYSALADOQUESEPRESENTASEELLAENLACERCANACASADECESP
EDESDICIENDOQUEHICIERANELFAVORDEDARLEUNDUROSIQUIERASELODIESENAPR
ESTAMOSEGURAMENTESEREIRIANDETANABSURDAPRETENSIONYLAPONDRIANBONI
TAMENTEENLACALLEYNOOBSTANTENATURALYJUSTOPARECIAQUEENCUALQUIERPA
RTEDONDEUNDURONOREPRESENTABAMASQUEUNVALORINSIGNIFICANTESELODIES
ENAELLAPARAQUIENLATALSUMAERACOMOUNATOMOINMENSO

Tipo de cifrado: Sustitución Monoalfabeto.
Clave:

Procedimiento de descifrado:



Lo primero que podemos ver es que la O y la Y son las letras con mas apariciones en el texto, basándonos en esto:

1. O -> E?, A? (incluso la propia O?)
2. Y -> A?, E? (incluso O?)
3. D -> O?
4. E -> S?,R?,N?
5. P ->S?,R?,N?
6. V -> S?, R?, N?

Después de una exploración manual de todas las combinaciones disponibles propuestas encontramos que lo que más se adapta y cobra sentido en el texto es:

En esta ventana, los caracteres del texto cifrado se representan con letras minúsculas mientras que los caracteres del texto claro son representados por letras mayúsculas (ejemplo: a --> C significa que la letra 'a' se sustituye (descifra) por una 'C').
Cada cambio realizado en la lista de sustitución será representado automáticamente en el cuadro inferior para comprobar los resultados.

a:	*	b:	*	c:	*	d:	O	e:	N	f:	*	g:	*
h:	*	i:	*	j:	*	k:	*	l:	*	m:	*	n:	*
o:	A	p:	S	q:	*	r:	*	s:	*	t:	*	u:	*
v:	R	w:	*	x:	*	y:	E	z:	*				

nONESEfuRARcAwOsiuShRAuiOtjEESENkOSfOfENhOSiEuNhENSAAfARwjRAnOfOjNwuR

OANwjShuOSOiEkAkfASOmRESufuSfAcEuAxASARxORjNAsOhRAmANiAiEkbARiuNwENh
ESxRESjROSASOuNiOkENhESjNOSkkEcAmANjNijROOhROSumANAmjSnARkOxASAmAN
nOmRAiORESiEkmANnOnONEkhAkEwjukkOAkzOfmROnARRunOnzESnONmOhEkkASiEn
ERcEqAswASEOSAnARROSljNEmRESENEknjAkERAnONijnuiOAknEfENhERuOAkwjNOAtj
uENNAiAufxORhAmANsAkOSijROSENkAShuENiASENhRAmANnOfxRAiORESTjESAkuANn
ONxAtjEhESfENiuwOSzARAxOSOSufxORhjNAmANA**kOSSENORES**nONRAxuiAcuSuONm
ENuNAxASOREcuShAkOSnAbONESiEhANhAhuENiAAkOSiuShuNhOSnjARhOSiEhOiASkA
SnASASAkOSmOkSukkOSiEhOiOShRANSEjNhESmuENcEShuiOSAitjuRuENiOkAnERhuijf
mREiEtjEENNuNwjNOiEAtjEkkOSRExkuEwjESiEkAcuiAlAkhAmAjNijROiESxjESxENSOtjES
ERuAjNxASOfjsSAkAiOtjESExRESENhASEEkkAENkAnERnANAnASAiEnESxEiESiunuENiO
tjEzunuERANEklAcORiEiARkEjNijROSutjuERASEkOiuESENAxREShAfOSEwjRAfENhESER
EuRuANiEhANAmSjRiAxREhENSuONskAxONiRuANmONuhAfENhEENkAnAkkEs**NOOmSh
ANhE**NAhjRAksbjShOxAREnuAtjEENnjAktjuERxARhEiONiEjNijRONORExRESENhAmAfASt
jEjNcAkORuNSuwNulunANhESEkOiuESENAEkkAxARAtjuENkAhAkSjfAERAnOfOjNAhOfOu
NfENSO

Viendo las dos cadenas de texto señaladas en el paso intermedio de la deducción, podemos notar que K -> L descifrada (kOSSENORES -> LOSSENORES) y que NOOmShANhE -> NOOBSTANTE, Ver dos O juntas hace sospechar.

nONESEfuRARcAwOsiuSTRAuiOtjEESENLOSfOfENTOSiE**uNTENSA**AfARwjRAnOfOjNwuR
OANwjSTuOSOiELALfASOBRESufuSfAcEuAxASARxORjNAsOTRABANiAiELbARiuNwENT
ESxRESjROSASOuNiOLENTESjNOSLLEcABANjNijROOTROSuBANABjSnARLOxASABAN
nOBRAiORESiELBANnOnONELTALEwjuLLOALzOfBROnARRunOnzESnONBOTELLASiEnE
RcEqAswASEOSAnARROSljNEBRESENELnjALERAnONijnuiOALnEfENTERuOALwjNOAtju
ENNAiAufxORTABANsALOSijROSENLASTuENiASENTRABANnOfxRAiORESTjESALuANnO
NxAtjETESfENiuwOSzARAxOSOSufxORTjNABANALOSSENORESnONRAxuiAcuSuONBEN
uNAxASOREcuSTALOSnAbONESiETANTATuENiAALOSiuSTuNTOSnjARTOSiETOiASLASn
ASASALOS**BOLSuLLOS**iETOiOSTRANSEjNTESBuENcESTuiOSAitjuRuENiOLAnERTuijfBR
EiEtjEENNuNwjNOiEAtjELLOSRExLuEwjESiELAcuiAlALTABAjNijROiESxjESxENSOtjESERu
AjNxASOfjsSALAiOtjESExRESENTASEELLAENLAnERnANAnASAiEnESxEiESiunuENiOtjEz
unuERANELlAcORiEiARLEjNijROSutjuERASELOiuESENAxRESTAfOSEwjRAfENTESEREu
RuANiETANABSjRiAxRETENSuONsLAxONiRuANBONuTAfENTEENLAnALLEsNOOBSTAN
TENATjRALsbjSTOxAREnuAtjEENnjALtjuERxARTEiONiEjNijRONORExRESENTABAfAStjEj
NcALORuNSuwNulunANTESELOiuESENAELLAxARAtjuENLATALSjfAERAnOfOjNATOfOuNf
ENSO

N-> C descifrada
U-> I descifrada

CONESEfIRARcAwOsiISTRAIiOtjEESEN**LOS-fOfENTOS-iE-INTENSA**-AfARwjRACOfOjNwI
ROANwjSTIOSOiELALfASOBRESIfISfAcEIAxASARxORjNAsOTRABANiAiELbARiINwENTE
SxRESjROSASOINiOLENTESjNOSLLEcABANjNijROOTROSIBANABjSCARLOxASABANCO
BRAiORESiELBANCOCONELTALEwjILLOALzOfBROCARRICOCzESCONBOTELLASiECER

cEqAswASEOSACARROSljNEBRESENELCjALERACONijCIiOALCEfENTERIOALwjNOAtjIE
NNAiAIfxORTABANsALOSijROSENLASTIENiASENTRABANCOfxRAiORESTjESALIANCONx
AtjETESfENiIwOSzARAxOSOSIfxORTjNABANALOSSENORESCONRAxIiAcISIONBENINAx
ASOREcISTALOSCAbONESiETANTATIENiAALOSiISTINTOSCjARTOSiETOiASLASCASAS
ALOSBOLSILLOSiETOiOSTRANSEjNTESBIENcESTIiOSAitjIRIENiOLACERTIijfBREiEtjEEN
NINwjNOiEAtjELLOSRExLIEwjESiELAcIiAlALTABAjNijROiESxjESxENSOtjESERIAjNxASOfjs
SALAiOtjESExRESENTASEELLAENLACERCANACASAiECESxEiESiICIENiOtjEzICIERANE
LIAcORiEiARLEjNijROSItjIERASELOiIESENAxRESTAfOSEwjRAfENTESEREIRIANiETANAB
SjRiAxRETENSIONsLAxONiRIANBONITAfENTEENLACALLEsNOOBSTANTENATjRALsbjST
OxARECIAtjEENCjALtjIERxARTEiONiEjNijRONORExRESENTABAfAStjEjNcALORINSIwNIII
CANTESELOiIESENAELLAxARAtjIENLATALSjfAERACOfOjNATOfOINfENSO

En esa secuencia podemos ver que I->D y que F-M para formar la palabra “momentos”.

CONESEMIRARcAwOsDISTRAIDOtjEESENLOSMOMENTOSDEINTENSAAMARwjRACOM
OjNwIROANwjSTIOSODELALMASOBRESIMISMAcEIAxASARxORjNAsOTRABANDADELbA
RDINwENTESxRESjROSASOINDOLENTESjNOSLLEcABANjNDjROOTROSIBANABjSCARL
O-**xASABAN-COBRADORES-DEL-BANCO-**CONELTALEwjILLOALzOMBROCARRICOCzE
SCONBOTELLASDECERcEqAswASEOSACARROSljNEBRESENELCjALERACONDjCIDOA
LCEMENTERIOALwjNOAtjIEN**NADA-IMxORTABAN**sALOSDjROSENLASTIENDASENTRAB
ANCOMxRADORESTjESALIANCONxAtjETESMENDIwOSzARAxOSOSIMxORTjNABANALO
SSENORESCONRAxIDAcISIONBENINAxASOREcISTALOSCAbONESDETANTATIENDAAL
OSDISTINTOSCjARTOSDETODASLASCASASALOSBOLSILLOSDETODOSTRANSEjNTES
BIENcESTIDOSADtjIRIENDOLACERTIDjMBREDEtjEENNINwjNODEAtjELLOSRExLIEwjESD
ELAcIDAIALTABAjNDjRODESxjESxENSOtjESERIAjNxASOMjsSALADOtjESExRESENTASE
ELLAENLACERCANACASADECESxEDESDICIENDOtjEzICIERANELIAcORDEDARLEjNDjR
OSItjIERASELODIESENAxRESTAMOSEwjRAMENTESEREIRIANDETANABSjRDAxRETEN
SIONsLAxONDRIANBONITAMENTEENLACALLEsNOOBSTANTENATjRALsbjSTOxARECIAt
jEENCjALtjIERxARTEDONDEjNDjRONORExRESENTABAMAStjEjNcALORINSIwNIIICANTE
SELODIESENAELLAxARAtjIENLATALSjMAERACOMOjNATOMOINMENSO

Podemos ver claramente que X -> P descifrada.

CONESEMIRARcAwOsDISTRAIDOtjEESENLOSMOMENTOSDEINTENSAAMARwjRACOM
OjNwIRO**-ANwjSTIOSO-DEL-ALMA-SOBRE-SI-MISMA-cEIA-PASAR-POR**-jNAsOTRABAN
DADELbARDINwENTESPRESjROSASOINDOLENTESjNOSLLEcABANjNDjROOTROSIBAN
ABjSCARLOPASABANCOBRADORESDELBANCOCONELTALEwjILLOALzOMBROCARRIC
OCzESCONBOTELLASDECERcEqAswASEOSACARROSljNEBRESENELCjALERACONDjC
IDOALCEMENTERIOALwjNOAtjIENNADAIMPORTABANsALOSDjROSENLASTIENDASENT
RABANCOMPRADORESTjESALIANCONPAtjETESMENDIwOSzARAPOSOSIMPORTjNABA
NALOSSENORESCONRAPIDAcISIONBENINAPASOREcISTALOSCAbONESDETANTATIEN
DAALOSDISTINTOSCjARTOSDETODASLASCASASALOSBOLSILLOSDETODOSTRANSEj
NTESBIENcESTIDOSADtjIRIENDOLACERTIDjMBREDEtjEENNINwjNODEAtjELLOSREPLIE
wjESDELAcIDAIALTABAjNDjRODESPjESPENSOtjESERIAjNPASOMjsSALADOtjESEPRESE
NTASEELLAENLACERCANACASADECESPEDESDICIENDOtjEzICIERANELIAcORDEDARL
EjNDjROSItjIERASELODIESENAPRESTAMOSEwjRAMENTESEREIRIANDETANABSjRDAP
RETENSIONsLAPONDRIANBONITAMENTEENLACALLEsNOOBSTANTENATjRALsbjSTOP

ARECIAtjEENCjALtjIERPARTEDONDEjNDjRONOREPRESENTABAMAStjEjNcALORINSIwNI
IICANTESELODIESENAELLAPARAtjIENLATALSjMAERACOMOjNATOMOINMENSO

Al leer “del alma sobre si misma” detectamos que el texto sea probablemente muy “lirico” por lo que ANGUSTIOSO nos encajaba perfectamente en el sentido literario del texto, por lo tanto W -> G descifrada y J -> U descifrada.

CONESEMIRARcAGOsDISTRAIDOtUEESENLOSMOMENTOSDEINTENSAAMARGURACO
MOUNGIROANGUSTIOSODELALMASOBRESIMISMA**cEIA**PASARPORUNAsOTRABANDA
DELbARDINGENTESPRESUROSASOINDOLENTESUNOSLLEcABANUNDUROOTROSIBA
NABUSCARLOPASABANCOBRADORESDELBANCOCONELTALEGUILLOALzOMBROCAR
RICOCzESCONBOTELLASDECERcEqAsGASEOSACARROSIUNEBRESENELCUALERAC
ONDUCIDOALCEMENTERIOALGUNOAtUIENNADAIMPORTABANsALOSDUROSENLASTI
ENDASENTRABANCOMPRADOREStUESALIANCONPAtUETESMENDIGOS**zARAPOSOS**I
MPORTUNABANALOSSENORESCONRAPIDAcISIONBENINAPASOREcISTALOSCAbONE
SDETANTATIENDAALOSDISTINTOSCUARTOSDETODASLASCASASALOSBOLSILLOSDE
TODOSTRANSEUNTESBIEN**cESTIDOS**ADtUIRIENDOLACERTIDUMBREDE**tUE**ENNINGU
NODEAtUELLOSREPLIEGUESDELAcIDAIALTABAUNDURODESPUESPENSOtUESERIAU
NPASOMUsSALADOtUESEPRESENTASEELLAENLACERCANACASADECESPEDESDICIE
NDOtUEzICIERANELIAcORDEDARLEUNDUROSItUIERASELODIESENAPRESTAMOSEGU
RAMENTESEREIRIANDETANABSURDAPRETENSIONsLAPONDRIANBONITAMENTEENL
ACALLEsNOOBSTANTENATURALsbUSTOPARECIAtUEENCUALtUIERPARTEDONDEUND
URONOREPRESENTABAMAStUEUNcALORINSIGNIIICANTESELODIESENAELLAPARAtUI
ENLATALSUMAERACOMOUNATOMOINMENSO

Con este fragmento ya muy claro y fácilmente interpretable nos basta para completar las letras restantes y descifrar el texto, siendo esta la Clave resultado:

6. Reto de Vigenere

Para este ejercicio hemos escogido el archivo 1.4_fragmento3_cif.txt y para ayudarnos en el criptoanálisis realizamos un script en python que nos automatice los apartados de cálculos y búsqueda de substrings que se repitan en el texto cifrado.
De este modo hemos buscado repeticiones de 4 y 5 caracteres que se repitan en el archivo, imprimiendo por pantalla la cadena en cuestión y las posiciones en las que se ubica. El resultado es siguiente:

Patrones repetidos de 4 caracteres y sus posiciones: {'GVJI': [7, 504], 'ZFLQ': [45, 871], 'PFUE': [92, 771], 'FUEV': [93, 772], 'STKT': [139, 923]}
Patrones repetidos de 5 caracteres y sus posiciones: {'PFUEV': [92, 771], 'JCOVA': [177, 338], 'COVAW': [178, 339], 'OVAWM': [179, 340], 'VAWMW': [180, 341]}

Aunque todas las cadenas aparecen un máximo de 2 veces vamos interpretar que al tratarse de una longitud relativamente grande, la posibilidad de que se repitan por pura casualidad es pequeña. En caso de que al avanzar en los cálculos para descifrar el texto veamos que no tienen sentido retrocederemos hasta este paso.
Ahora vamos a calcular las distancias entre cada cadena de caracteres y el mcd de la distancia entre todas las cadenas de longitud 4 y longitud 5 por separado, esto lo realizaremos con el script realizado, y el resultado es el siguiente:

Distancia para patrones de 4 caracteres: {'GVJI': 497, 'ZFLQ': 826, 'PFUE': 679, 'FUEV': 679, 'STKT': 784}
Distancia para patrones de 5 caracteres: {'PFUEV': 679, 'JCOVA': 161, 'COVAW': 161, 'OVAWM': 161, 'VAWMW': 161}
MCD de todas las distancias para patrones de 4 caracteres: 7
MCD de todas las distancias para patrones de 5 caracteres: 7

Una vez realizados los cálculos llama la atención que el mcd para las distancias de ambos vectores de subfragmentos es igual a 7, de modo que vamos tomar este número como la longitud de la clave, y para continuar, dividiremos el texto en fragmentos con esta extensión para luego sacar los carácteres que pertenecen a la misma posición dentro de cada cadena e imprimirlos en un mismo vector, de este modo la salida obtenida sería la que se muestra a continuación:

Grupos de caracteres en posición 1 :

VGWVQORQJTGAJUKTNUAETCFXUQWTAGPEQWUOUZGNPGENCTAWSWWDQGECNC
WNKCTKGJHIPFNCGGWUGQUPXVGJGOCOCGGPNWQQPCFTTXQNQQEKCPQPCFNKQ
PCGOWUCKCGUPGEGTVGEPKGUGGSOCVTPV

Grupos de caracteres en posición 2 :

ZVVMKQMCMMVAMPDBWLBWKAMWWLMITBABMVAMBWVQLJBILKAZCMMIAQIZDDHMV

CLOTIMZBQWLVOMBAUIBQCUIAQZILVZVMAZAWBQQWIUZAAMIABPAKIMKITTOQMMUOJ
VQDGBXKWTCAMAMVRCJJZMIQ

Grupos de caracteres en posición 3 :

FJIWTSHSHUYZWFNFXNZVTZQXGJWLZFZJSHJSTWQEJJZRJJJFJWJSHSJFNJISTSJTTG
SFJTXTJZRJJJYTIRGIZLFSNYJFERYMXFTGSIGJRFJXIFFZTJHTNFTTJFSJSFTGNUFZTFF
QNWYFYJJWFTQIJ

Grupos de caracteres en posición 4 :

JIFIDZZRYRIJDUFUUFMLEEFTVCKIXETIJZMKVRRRJIRRLCRSCKEVLFJEVIVJYCTUJZUM
RJDJIERIIKFVRRRVEFQRTVEKRRLVJUJCFFIPLGEWZJUWEEKFUVJJIZTEZVVCJVDUILVR
XKFIFDVVGCRFI

Grupos de caracteres en posición 5 :

OESAOOFVOREDAEAOESOELTSOROOAUTACUOEEIBRCUEBNNESAOOTNRNCYRLLUA
UAOQAIELEAEAESIAIRNPSRSEDANADTUDSNREETEMEEDEAVOSCEOODOCEPGAODIT
FLSEIREORNSCAAQGPPLEOACCR

Grupos de caracteres en posición 6 :

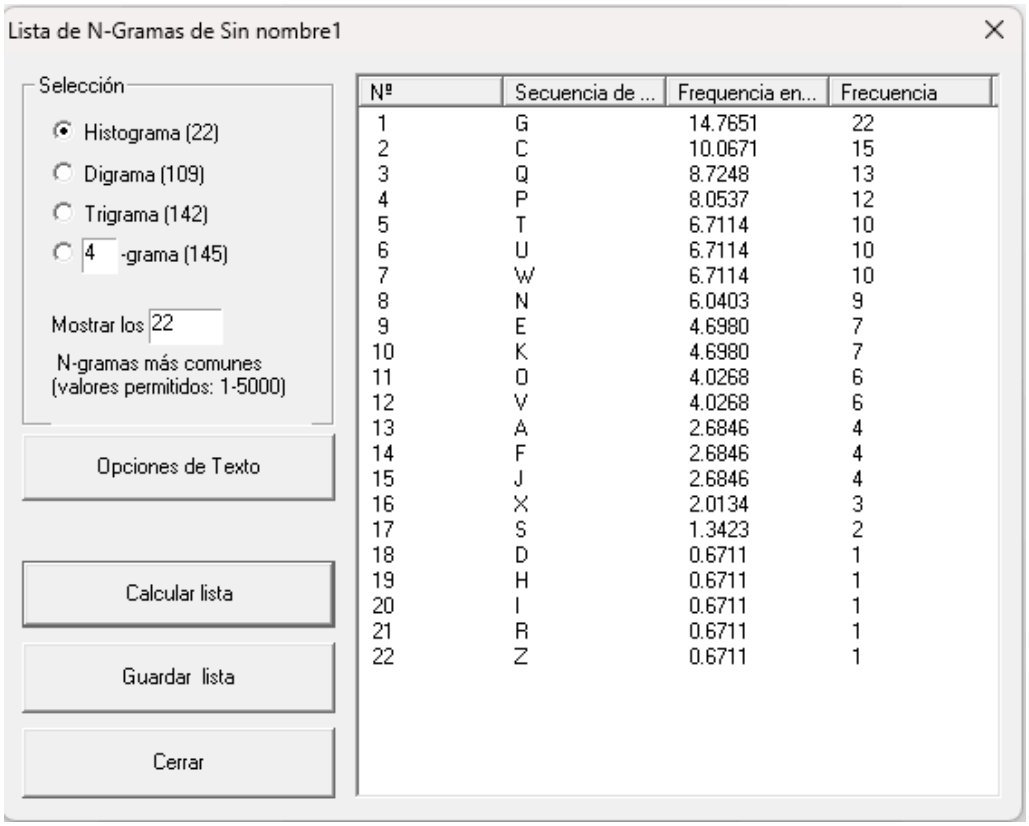
EOXQGHLHHWHRQVSGPHSYRRYPDVVYERURVQUMQOHLVVDHFUHGVVUVRXDYDDVU
EJVQXQGPRVOQOVSRQGPORLJQQHKLOLHUHDDPWXHSDOGHUUDUWRVUFLDRVLUV
QHOHLTYREIQVHTSLDSXXROQVUGLRD

Grupos de caracteres en posición 7 :

HAPSCGQNZCZGCJOSOGCSGGWCBASSFSOATSOISSOCROOFOCUSAEOIFBDCBZCSW
OHRSCCSGMJUGECFGCSOGBCCSZIFATSOGTROFBFSZBSZHSFAWASAWOHASQWIEGZ
GQIWWZSHSQISCPISAFCCHCCCB

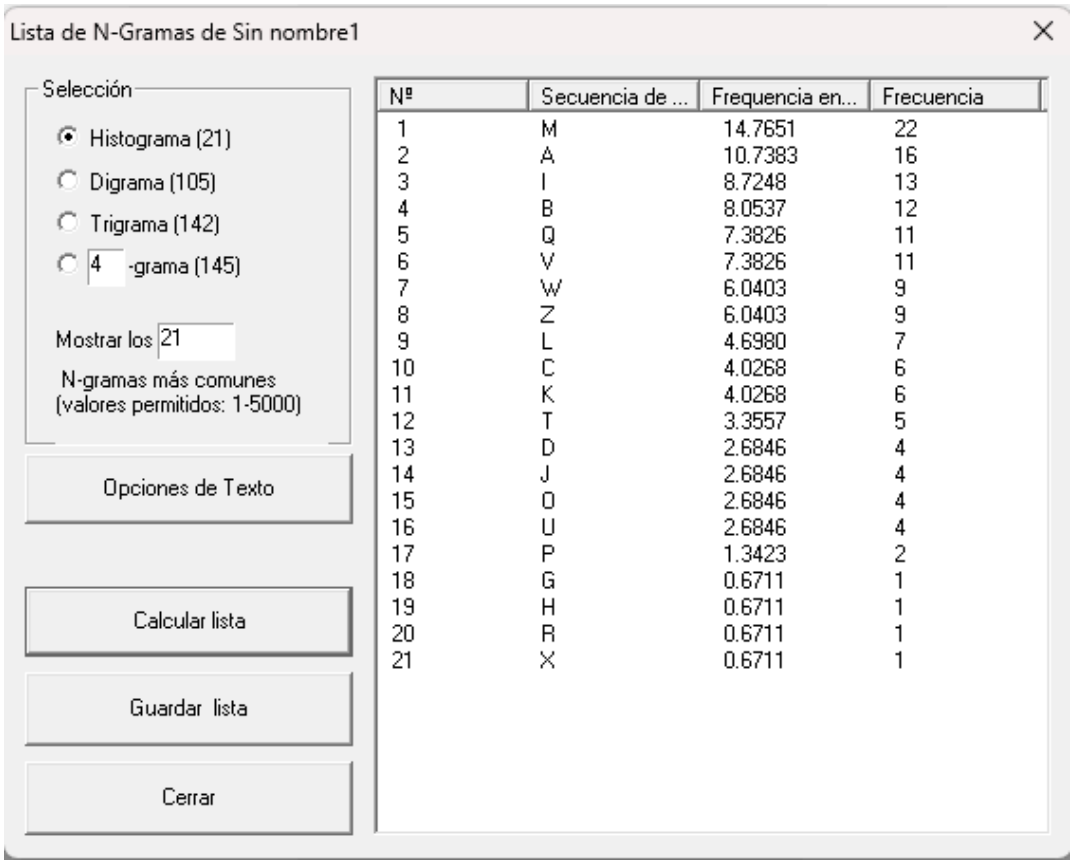
Llegados a este punto podemos usar cryptool para hacer el análisis de frecuencias de cada uno de los fragmentos y, mediante la técnica AEOS, asignar a cada letra cifrada su correspondiente en texto plano y obtener el desplazamiento de cada subcriptograma.

Para los caracteres de la posición 1 obtenemos el siguiente análisis de frecuencias:



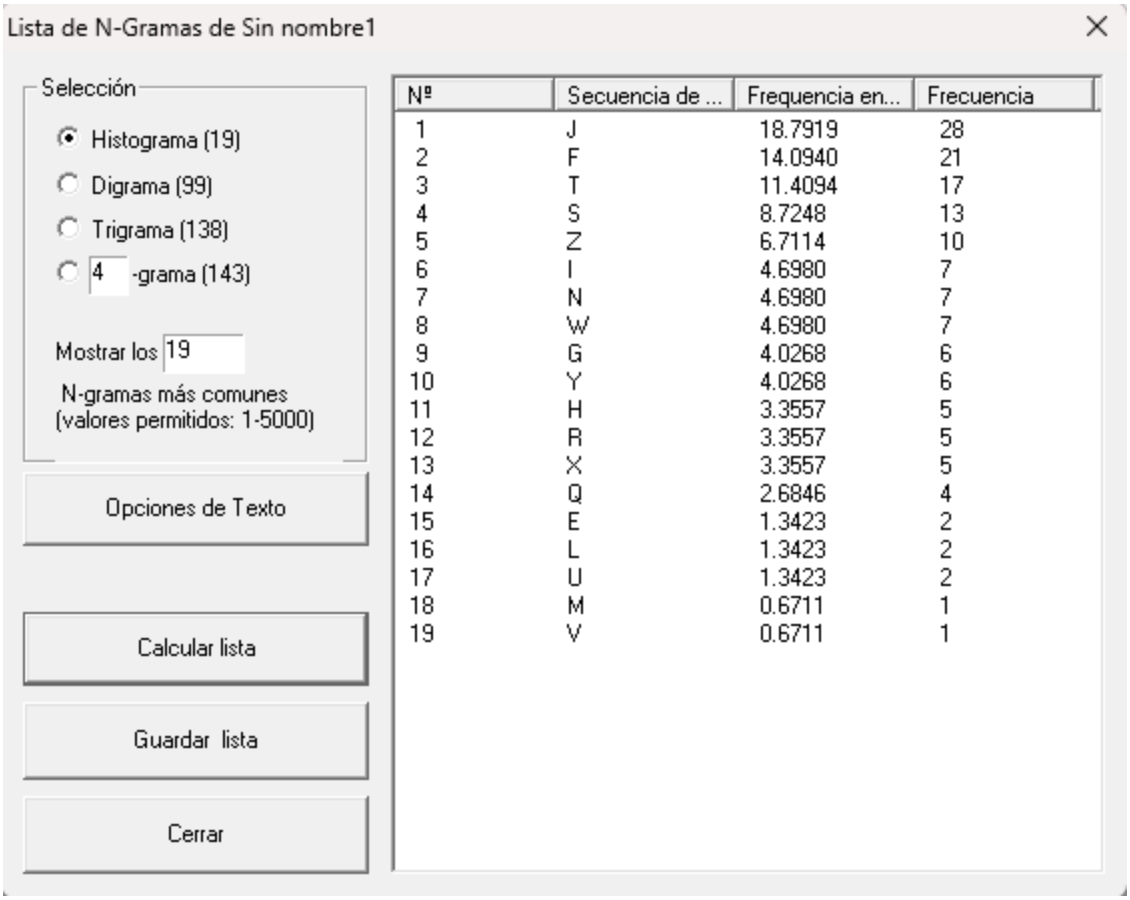
Analizando el resultado obtenido, donde las letras mas frecuentes son la G y la C, podemos darnos cuenta que la distancia entre ambas es 4, la misma que entre la letra A y la E en el abecedario. De este modo llegamos a la conclusión de que la C cifrada equivale a la A, obteniendo como resultado un desplazamiento de +4 en la primera posición de la clave.

Ahora pasaremos al grupo de caracteres en posición 2, obteniendo el siguiente resultado del análisis:



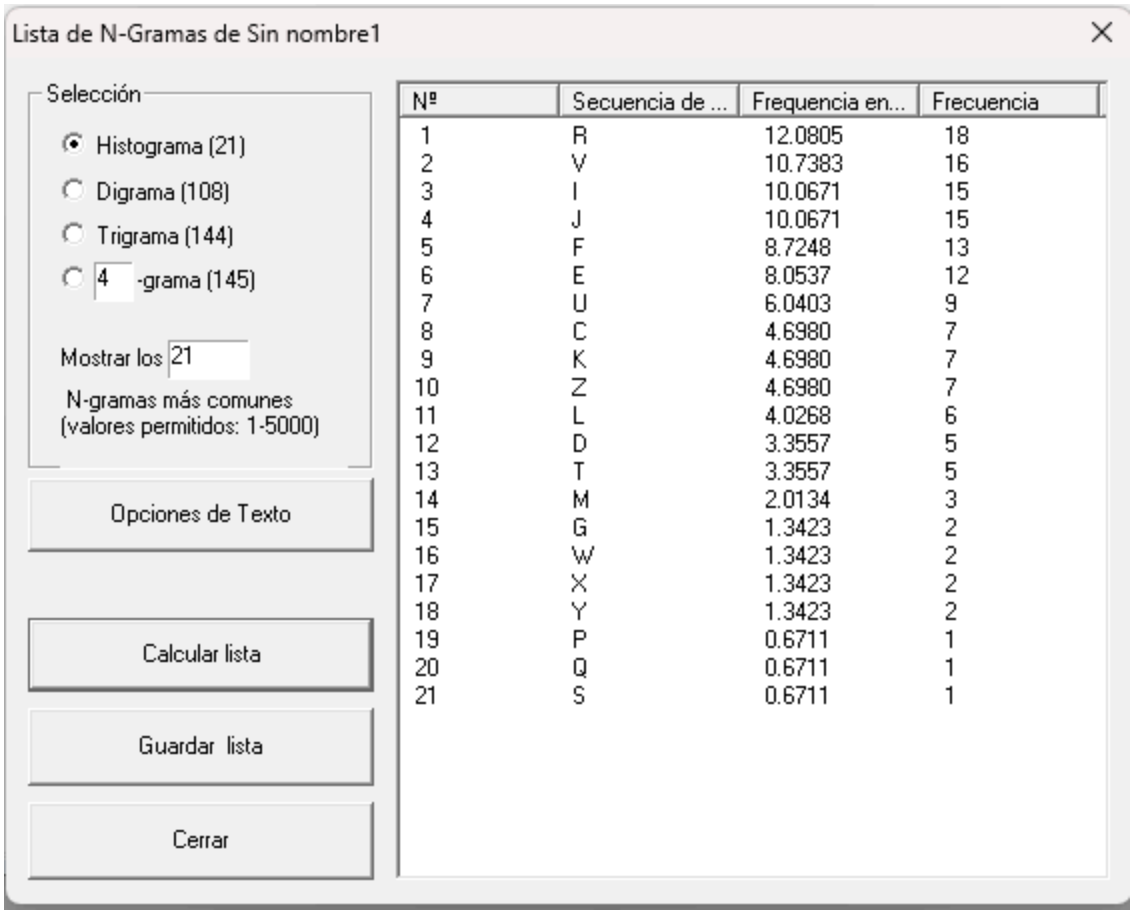
En este caso la letra con mayor número de apariciones es la M, y si aplicamos la regla +4 para obtener la E cifrada vemos que la tercera letra más frecuente del texto, I, con desplazamiento +4 es M, por lo que la I cifrada equivale a la A en el texto plano.

Continuamos con la posición 3:



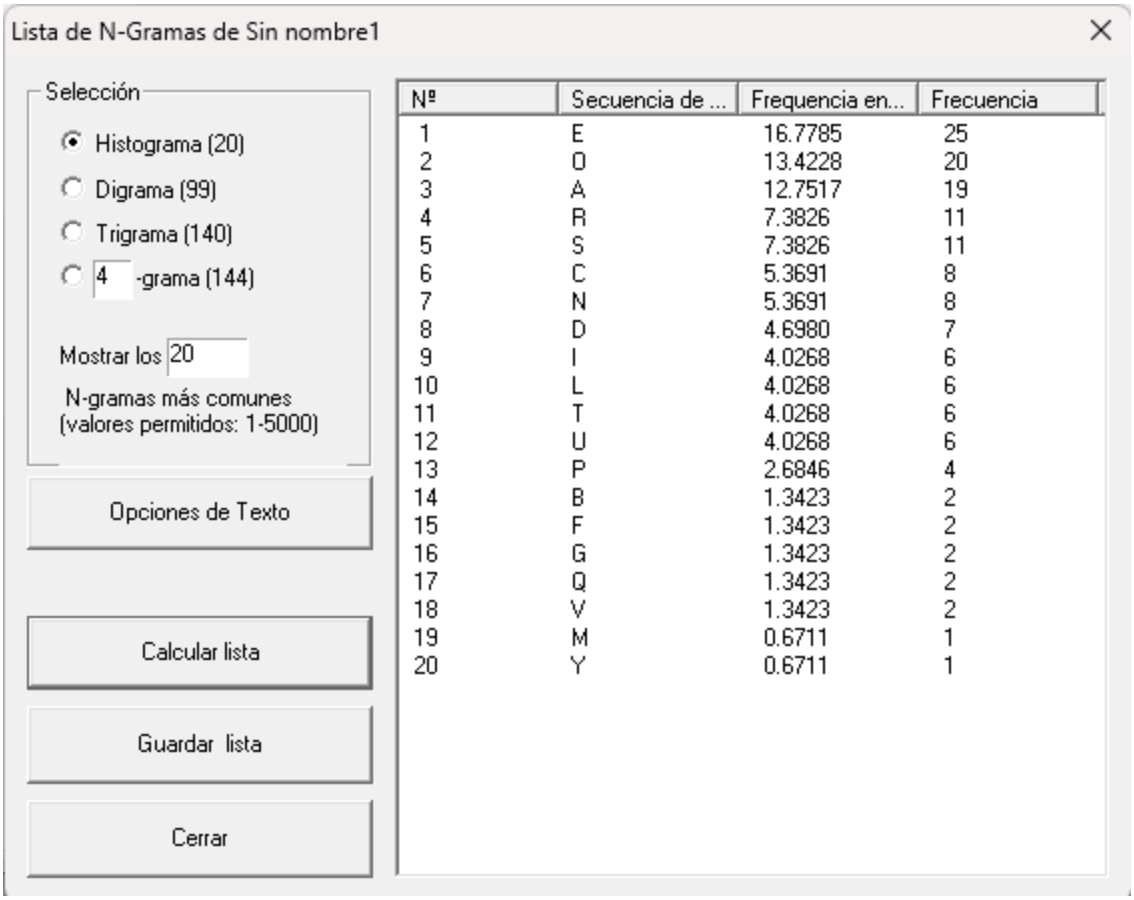
En este caso la letra F con desplazamiento +4 es la J, ambas las más frecuentes en el fragmento, por lo que la F equivale a la A en texto plano.

Ahora la posición 4:



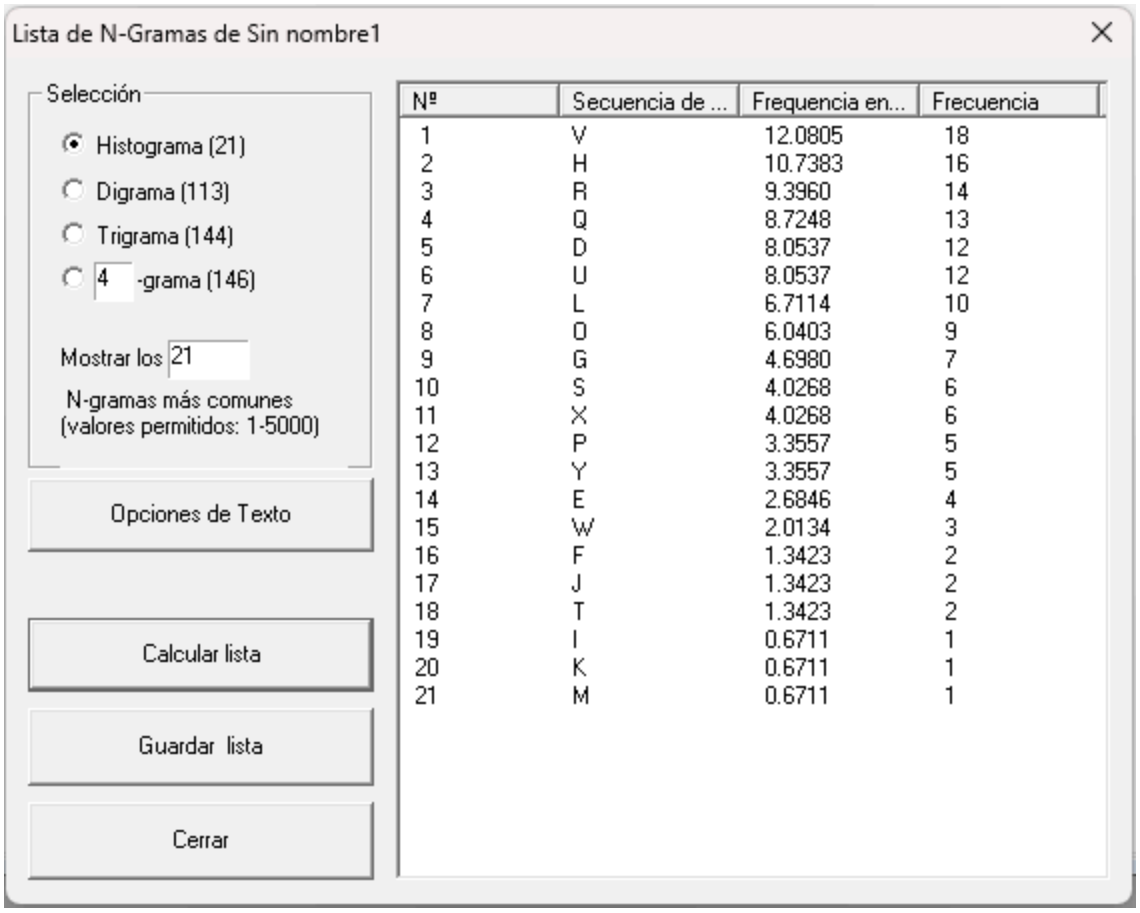
Para este fragmento el análisis es sencillo, pues las dos letras más frecuentes cuentan con un desplazamiento de 4 de la primera sobre la segunda, de tal modo que la R es el resultado que estamos buscando.

Continuamos con el 5 fragmento:



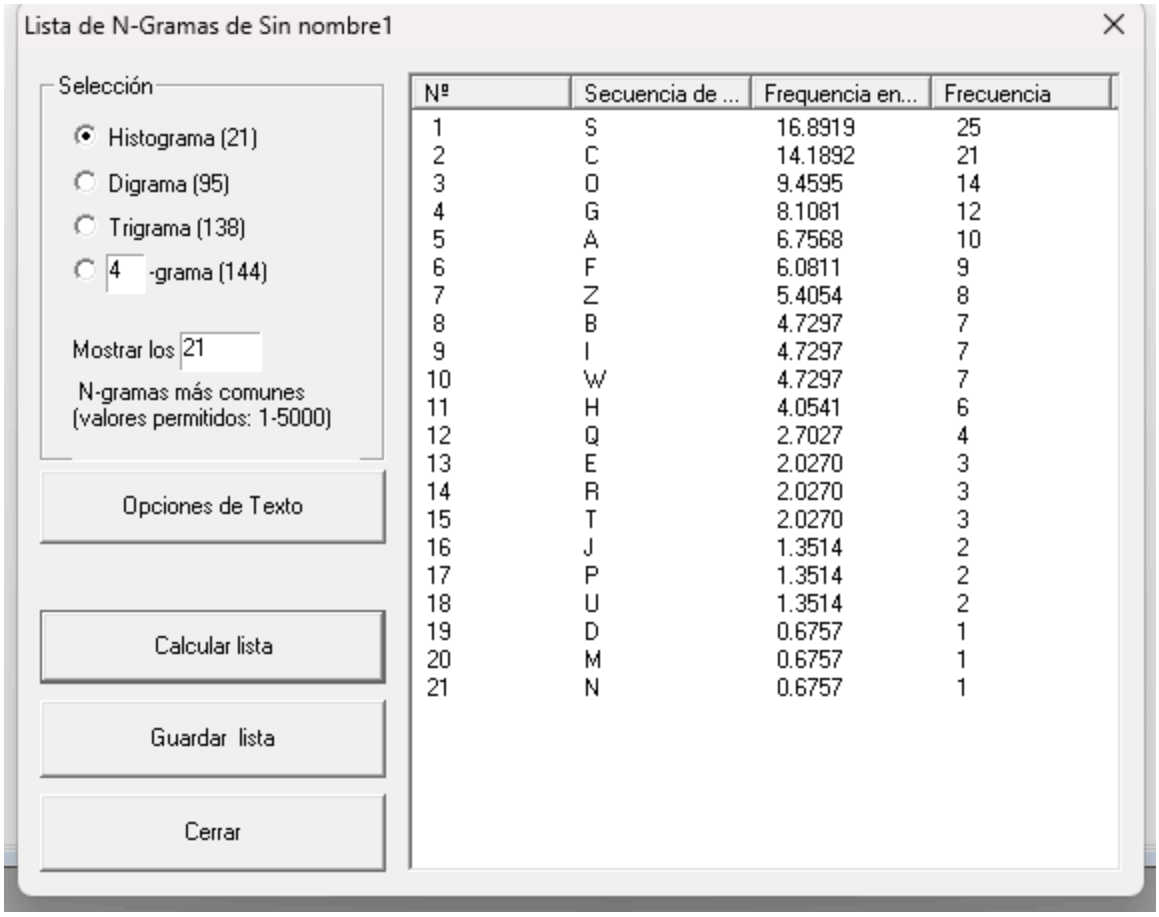
Las letras más frecuentes son las vocales E, O y A, habiendo una minima diferencia entre la segunda y tercera, pero con la diferencia que la A con desplazamiento 4 es la letra E. De este modo sabemos que este fragmento no varía entre el texto plano y el cifrado.

Sigamos con la penúltima posición, sabiendo que hasta ahora la clave es `CIFRA` a falta de los dos últimos caracteres.



En esta ocasión debemos observar detenidamente, pues no hay una candidata clara, tanto puede ser la H y la L el par buscado o la D y la H, ambas podrían ser coherentes, aunque por el número mayor de apariciones del par en conjunto, vamos tomar como que la D cifrada es la A en el texto plano y la H (su correspondiente con desplazamiento 4) es la E.

Llegados a este punto pensamos que la clave, a falta del último carácter, es CIFRAD, lo que nos hace pensar que esa última letra que nos falta puede ser la O, dando como clave la palabra CIFRADO. Vamos a verlo en el análisis de frecuencias si nuestra hipótesis se cumple:



Sobre el análisis vemos que el desplazamiento buscado puede ser tanto el par O-S como el par C-G, ambos son similares en número de apariciones y cumplen con nuestra condición de desplazamiento 4 para obtener la A y la E del texto plano.

Tal y como mencionamos antes creemos que la clave es CIFRADO, siendo la última letra la O, que coincide con uno de nuestros candidatos del análisis de frecuencia. Vamos a comprobar en cryptool si al intentar descifrar el texto con nuestra clave se obtiene una cadena con sentido.

El resultado obtenido es el siguiente:

TRASOBTENERELMUNDOSUBTERRANEOCOMODOMINIOESPECIFICOUNAVEZHECHOEL
REPARTOENTREELYSUSDOSHERMANOSHADESVIVIOAPARTADODELOSDEMASDIOSES
YTUVOPOCOQUEVERCONLOSASUNTOSDELOSVIVOSCOMOSOBERANODELOSMUERTO
SERAGRAVEYLUGUBRETANTOENSUCARACTERCOMOENSUSFUNCIONESSEVERAMENT
EJUSTOEINEXORABLEENLAREALIZACIONDESUSDEBERESACTUABAALAMANERADEUN
CARCELEROYSEASEGURABADEQUELOSMUERTOSQUEENTRABANENSUOSCUROREIN
ONUNCAESCAPARANYVOLVIERANAVERLALUZDELSOLENSUREINOHABIAUNLUGARDEC
ASTIGODONDELOSQUEHABIANOFENDIDOGRAVEMENTEALOSDIOSESYLOSMALVADOS
ENGENERALSEGUNESQUEMASPOSTERIORESERANSOMETIDOSATORMENTOENLAVIDA

POSTUMASINEMBARGOHADESNOESUNENEMIGODELARAZAHUMANANIRADICALMENT
EDIFERENTEENNATURALEZADESUSMASAFORTUNADOSHERMANOSSETRATADEUNDIO
STERRIBLEPERONOMALVADOELNOMBREDELREYDELOSMUERTOSAPARECEENVARIAS
FORMASDISTINTASCOMOHADESENSUFORMACONOCIDAENDIALECTOATICOOCOMOAI
DESENLAEPICALOSGRIEGOSASUMIERONQUEAIDESSENCILLAMENTESIGNIFICABAELQ
UENOESVISIBLEOINVISIBLEYPERFECTAMENTEPUDOSERCORRECTOAUNQUELAESPEC
ULACIONSIGAABIERTAPUESTOQUESEARGUMENTOPOREJEMPLOQUEELNOMBREESTA
BAPOROTROLADORELACIONADOCONTIERRA

Se ve que el texto tiene sentido, por lo que efectivamente la clave del mismo es la palabra CIFRADO, con longitud 7, tal y como habíamos calculado inicialmente.

7. Implementación Kasiski

7.1 Explicación implementación

La implementación de kasisky se basa en dos partes principales, encontrar el tamaño de clave y encontrar la clave.

Encontrar el tamaño de clave se basa en el análisis de frecuencias y calculando el MCD de todas las coincidencias.

```python
def ataque_kasiski(texto_cifrado, longitud_min_repeticion):
    repeticiones = encontrar_repeticiones(texto_cifrado, longitud_min_repeticion)
    distancias = encontrar_distancias_entre_repeticiones(repeticiones)
    factores_comunes = encontrar_factores_comunes(distancias)
    longitud_clave=obtener_tamaño_clave(factores_comunes)
    return longitud_clave
```

7.2 Salida –help

Sintaxis: kasinski.py fichero.txt

8. Implementación RC4

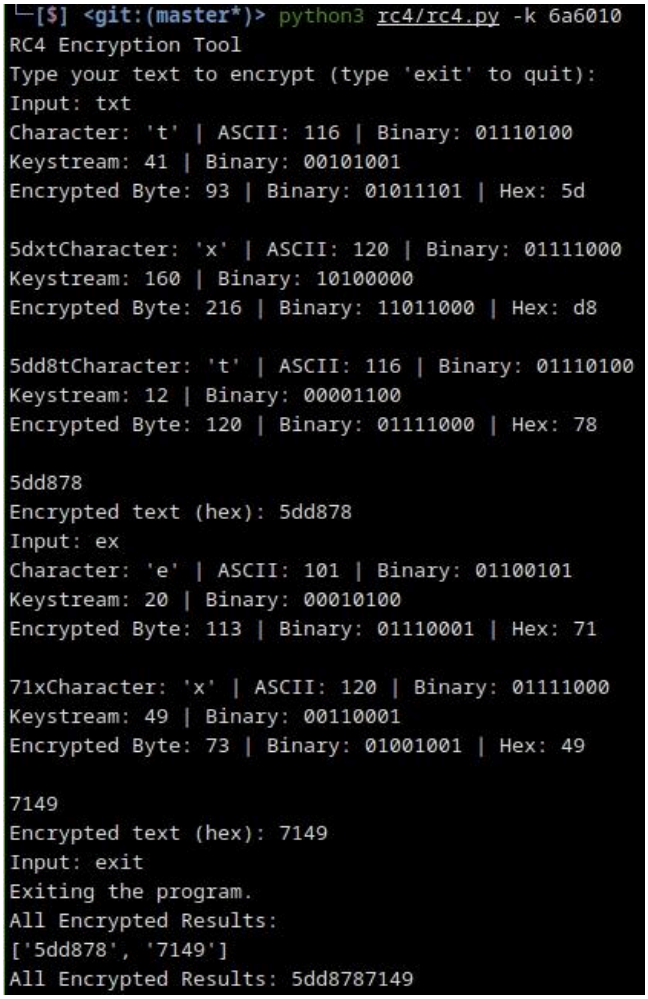
8.1 Salida -help

usage: rc4.py [-h] -k KEY [-d]

RC4 encryption tool

options:
  -h, --help   show this help message and exit
  -k KEY, --key KEY Hexadecimal encryption key
  -d, --decrypt   Decrypt mode (default is encrypt)

8.2 Evidencia correcta implementación



9. Principales diferencias entre DES y AES

9.1. Características Técnicas

Caracteristica	Cifrado DES	Cifrado AES	Comparativa
Clave	Utiliza una clave de 64 bits, aunque de estos solo utiliza como clave 56, el resto son bits de control. Conociendo este dato se deduce fácilmente que sus combinaciones totales son 2^56 (o lo que es lo mismo, unos 72 billones)	Tiene 3 posibilidades a usar dependiendo de los requerimientos en los que se aplique, estos 3 largos de clave distintos son 128 bits, 192 bits y 256 bits. Esto hace que sus combinaciones posibles mínimas para la clave sean 2^128 (340 undecillones).	Conociendo estos datos, y sabiendo que DES fue creado en 1970 y roto en 1999, mientras que AES (En la práctica) no es vulnerable a ataques de fuerza bruta, por lo tanto, este cambio en el tamaño de clave hace a AES mucho más resistente.
Tamaño de Bloque	Divide los datos en bloques de 64 bits.	Divide los datos en bloques de 128 bits.	Esta diferencia hace que un bloque de AES sea más seguro que uno de DES ya que es más resistente a un ataque de cumpleaños (ver anexo 1 del apartado). Además de eso AES, en la práctica, es mucho más rápido en sistemas modernos que DES y esto ocurre porque los procesadores actuales pueden manejar un volumen mayor de datos por ciclo de reloj, siendo 128 bits mucho más adecuado para una arquitectura moderna y en la que se cifran con mayor calidad grandes volúmenes de datos.
Tipo de algoritmo de cifrado	Red Feistel, en la que se realizan los siguientes pasos:	SPN (Red de Sustitución-Permutación) con varias operaciones las	La SPN utilizada por AES es más compleja que la red Feistel de DES y que incluso de 3DES pero aun

	1. Se pasa la mitad derecha **R(n-1)** a través de una función de expansión **E**, que la expande de 32 a 48 bits. 2. Se realiza un XOR entre el resultado expandido y la subclave de la ronda **K(n)**. 3. El resultado del XOR se pasa a través de 8 **S-boxes** predefinidas, que sustituyen los bits de entrada por otros bits (reduciendo los 48 bits a 32 bits). 4. El resultado se pasa por una permutación final **P**, esto permite el descifrado. 5. Finalmente, la mitad izquierda **L(n-1)** se intercambia con **R(n)** para la siguiente ronda, de modo que **L(n) = R(n-1)** y **R(n) = L(n-1) XOR f(R(n-1), K(n))**.	cuales son: 1.SubBytes: sustitución no lineal de bytes de acuerdo a la S-Box. 2.ShiftRows: Transposición de filas en la matriz que está siendo cifrada. 3. MixColumns: Operación de mezclado que combina los 4 bytes de cada columna de la matriz cifrada usando transformación lineal. 4. ArroundKey: Se genera una clave around en base a una iteración de la clave y se combina con la matriz a cifrar. (MixColumns no se realiza en la última iteración)	así los modos de operación influyen mucho en la efectividad de los cifrados. Todo esto no ha de ser visto como una comparación directa. DES fue un estándar muy útil y que trajo la criptografía “fuerte” al nivel general de usuario alla por 1970 pero que ya fue vulnerado mientras que AES, anunciado en el 2001, es una respuesta a el avance en la capacidad de computación de la tecnología moderna y una evolución significativa que que continúa resistiendo al paso de los años.
Número de rondas de cifrado	16 rondas de cifrado, todas basadas en red Feistel, que como sabemos opera dividiendo el mensaje original en bloques de tamaño igual (aplicando padding si es necesario), y con esa división se aplica una función F y un Intercambio de datos.	10, 12 o 14 rondas de fijado dependiendo del tamaño de la clave, incluyendo cada ronda sustitución, permutación y mezcla de datos, lo que aumenta la robustez, complejidad y difusión de la información.	Aunque 16 rondas de la red Feistel ofrecen seguridad para la época en la que se creó DES el hecho de que en AES cada ronda esté compuesta de más pasos internos y con una clave mayor hace que sea mucho más resistente.

Caja de Sustitución (S-box)	Cajas de sustitución fijadas, conocidas y relativamente simples, las cuales mapean 6 bits de entrada a 4 bits de salida en la red Feistel. DES usa 8 S-boxes durante el cifrado.	Cajas de sustitución no lineales, generadas usando el inverso multiplicativo en GF(2^8) con una transformación lineal de bits. Durante el cifrado se usa solamente una S-box, la cual tiene 8 bits de entrada y 8 de salida (1 Byte E/S).	Por lo tanto, podemos ver que las S-Boxes conocidas de DES introducen confusión, pero la S-Box de AES la introduce mucho más fuerte, al usar una operación matemática compleja que hace mucho mas difícil el criptoanálisis que en las S-Boxes fijadas de DES.

10. OpenSSL

10.1. Tiempo AES y DES

El comando a utilizar para cifrar con el algoritmo des usando una clave de 56bits es el siguiente:

openssl enc -des-cbc -in secreto.txt -out secreto_des.enc -K 0123456789abcdef -iv 0102030405060708 -provider legacy

Por su parte el comando para cifrar con aes y una clave de 256bits es:

openssl enc -aes256 -in secreto.txt -out secreto_aes.enc -K 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff -iv 0102030405060708090a0b0c0d0e0f10

El tiempo de ejecución para el algoritmo DES es de 19s y para AES-256 es 6s.

10.2. Modos ECB y CBC

El modo CBC es el usado por defecto por openSSL, por lo que en el apartado anterior ya lo hemos utilizado, ahora vamos a ver ECB.

Para DES el tiempo de ejecución en este modo es de 19s mientras que para AES-256 es de 7s, los comandos usados son los siguientes:

openssl enc -des-ecb -in secreto.txt -out secreto_des.enc -K 0123456789abcdef -provider legacy

openssl enc -aes-256-ecb -in secreto.txt -out secreto_aes.enc -K
00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff

Si analizamos los resultados obtenidos vemos que no hay gran diferencia de tiempo entre modos, esto se debe a que el archivo a cifrar es pequeño, pues CBC utiliza un vector de inicialización (IV) y cada bloque depende del anterior para ser cifrado dificultando paralelizar el cifrado de cada bloque, sin embargo ECB si permite cifrar cada bloque de forma independiente y por tanto permite la paralelización.

También debemos mencionar que en procesadores modernos las operaciones de CBC pueden estar aceleradas por hardware, reduciendo al mínimo la diferencia computacional entre este modo de trabajo y ECB.

10.3. Modos en OpenSSL

Si, estan disponibles los modos de operación ECB, CBC, CFB, OFB para DES y los modos ECB, CBC, CFB, OFB, CTR para AES-256

10.4. Tiempos AES vs DES

Por lo que vimos en los apartados anteriores usando el comando time AES es más rápido que DES, esto es debido a que los procesadores modernos cuentan con optimizaciones para el uso de cifrado AES, pero a nivel algoritmo DES también está menos optimizado que su contraparte.

10.5. Vulnerabilidades sobre AES

AES es vulnerable a ataques de canal lateral, estos se basan en tomar datos de la carga de cpu, consumo eléctrico o usos de cache entre otros. Actualmente se considera demasiado costoso realizar ataques de este tipo, por lo que AES sigue siendo seguro.

Otras formas de ataques sobre AES requerirían el uso del algoritmo en modos pocos seguros (ECB) o sistemas hardware con vulnerabilidades, un ejemplo es el ataque meltdown/spectre, el cual afecta a la memoria de la CPU llegando al punto de poder comprometer claves cifradas. También nos debemos asegurar que los IV sean aleatorios, pues el mismo vector puede generar patrones parecidos en la salida.

11. Simulación OpenSSL

11.1 Salida -help

```
usage: cipher.py [-h] [--key KEY] {encrypt,decrypt} {AES,DES} {ECB,CBC} input_file output_file

Encrypt or decrypt files using AES or DES

positional arguments:
  {encrypt,decrypt}  Action to perform
  {AES,DES}          Encryption algorithm
  {ECB,CBC}          Mode of operation
  input_file         Input file path
  output_file        Output file path

options:
  -h, --help         show this help message and exit
  --key KEY          Decryption key (hex format)
```