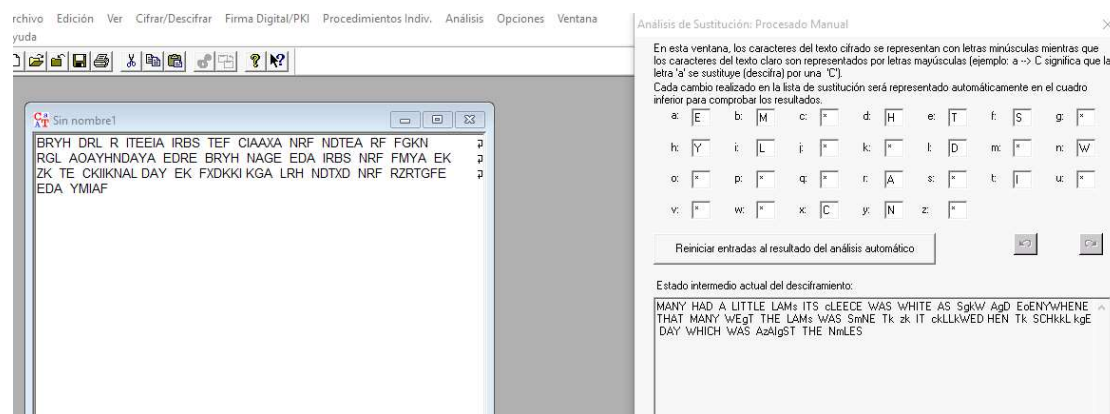


PRÁCTICA 2 SPSI - RAFAEL LACHICA GARRIDO

7) Descifrar los mensajes por sustitución y por Vignere/Schrodel.

Sustitución

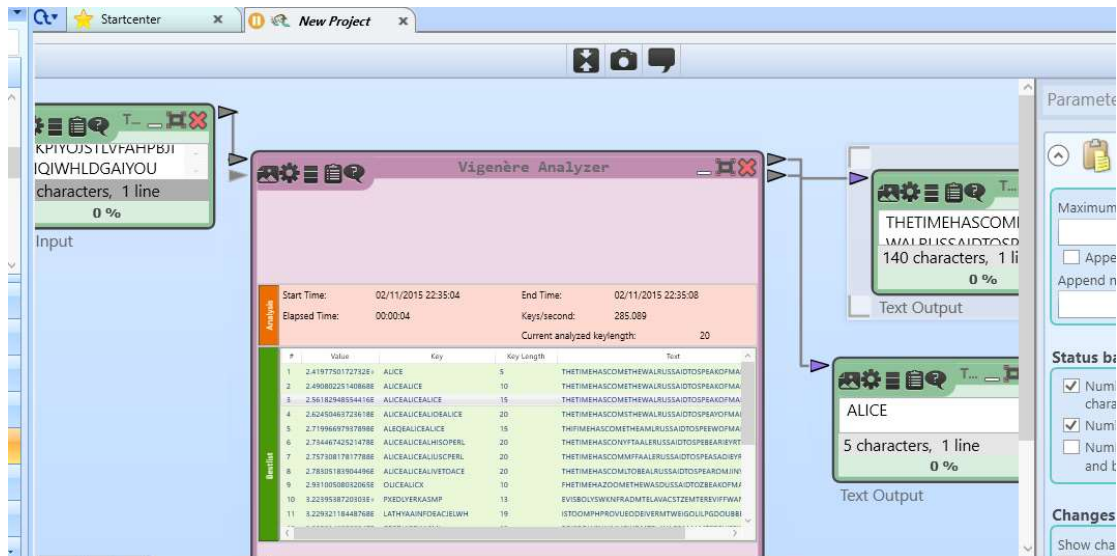


Sustituimos las letras y obtenemos el mensaje:

MARY HAD A LITTLE LAMB ITS FLEECE WAS WHITE AS SNOW AND EVERYWHERE
THAT MARY WENT THE LAMB WAS SURE TO GO IT FOLLOWED HER TO SCHOOL ONE
DAY WHICH WAS AGAINST THE RULES

Vignere

Seleccionamos cryptanalysis y obtenemos la clave **ALICE**



Clave: ALICE

Texto plano:

THETIMEHASCOMETHEWALRUSSAIDTOSPEAKOFMANYTHINGSOFSHOESANDSHIPSANDSEALINGWAXOFCABBAGE
SANDKINDSHGDWHYTHESEISBOILINGHOTANDWHETHERPFOEWWD BCAXQMQ

8) Análisis de cifrados Monoalfabéticos, Polialfabéticos, Enigma y Máquina Purple.

TEXTO LLANO

EL HOBBIT J.R.R Tolkien

En un agujero en el suelo vivía un Hobbit. No un agujero húmedo, sucio, repugnante, con restos de gusano y olor a fango, ni tampoco un agujero seco, desnudo y arenoso, sin nada en que sentarse o que comer: era un agujero hobbit, y eso significa comodidad.

Tenía una puerta redonda, perfecta como un ojo de buey, pintada de verde, con una manilla de bronce dorada y brillante, justo en el medio. La puerta se abría a un vestíbulo cilíndrico, como un túnel: un túnel muy cómodo, sin humos, con paredes revestidas de madera y suelos enlosados y alfombrados, provistos de sillas barnizadas, y montones y montones de perchas para sombreros y abrigos; el hobbit era aficionado a las visitas.

MONOALFABÉTICO

Clave: TOLKIEN

IF AJOOBS C.Q.Q Sjfdbih

Ih uht tnuciqj ih if ruifj vbvívt uh Ajoobs. Hj uh tnuciqj aúgikj, rulbj, qimunhthsi, ljh qirsjr ki nurthj y jfqj t ethnj, hb stgmjlj uh tnuciqj rilj, kirhukj y tqihjrj, rbh htkt ih pui rihstqri j pui ljgiq: iqt uh tnuciqj ajoobs, y irj rbnhbeblt ljgjbktk.

Sihít uht muiqst qikjhkt, miqeilst ljgj uh jcj ki oui, mbhstkt ki viqki, ljh uht gthbfft ki oqjhli kjqtkt y oqbffthsi, cursj ih if gikbj. Ft muiqst ri toqit t uh virsioufj lbfihkqblj, ljgj uh súhif: uh súhif guy lógikj, rbh augjr, ljh mtqikir qivirsbktr ki gtikiqt y ruifjr ihfjrtkjr y tfejgoqtjkr, mqjvbsjr ki rbfftr otqhbztkt, y gjsjhir y gjsjhir ki miqlatr mtqt rjgoqiajr y toqbnjr; if ajoobs iqt teblbjhtkj t ftr vbrbstr.

POLIALFABÉTICO - VIGNERE

Clave : TOLKIEN

XZ SYJFVM X.C.B BsydwpX

Mr hgo lqcnrkc px mp fnswy dmiíoo fx Psouwe. Xw ya tuftmbv aúapnw, whvwz, bmthzblxbi, phb coaxbl rp qcwngc j ytse t tlxos, ab hlwxspH iy koywxfz cmgb, wsdxchb r ocovsfh, gtx veqt sy aci fxbekzwr h efo kszxf: pbi ya tuftmbv acmlqx, l xgz cqkabttmi gbfcosleq.

Msyik crn iipbbe exrxle, cxfqokxn vcxy cr bcc oo jyrr, dtxbeqt rp fmvqx, qzx crn foystpn ws mbwrpx rzbihn r pcstpnghp, tcwgh sy ot qrwvz. Vi thxfek ai nufil k cr ixgeilcpb vwwxlvvvc, nyus hg húyot: ya múbpv uyl vóaznw, wvg vfwwww, phb akziqXg codifmwoka hr foooze l lipvwv rgzzcihbl m lvnszuflnww, ckcgSaxbl rp cqpytg mkzrvsooka, c zhbeyvif r azxbsaxg oo xievvlc xeet gzwjvrkcd i ifebuzc; mp uhpmsb iet oqskgvhblnw e ytg gsamgtg.

Podemos concluir que es mucho más fuerte que el cifrado monoalfabético de arriba en el que se toma una clave y se desplaza el alfabeto a raíz de la misma, ya que con ese simplemente tomando los mayores valores usados podemos obtener una correlación. Sin embargo, para Vignere necesitamos tener una clave y conocerla para poder descifrarlo.

ENIGMA

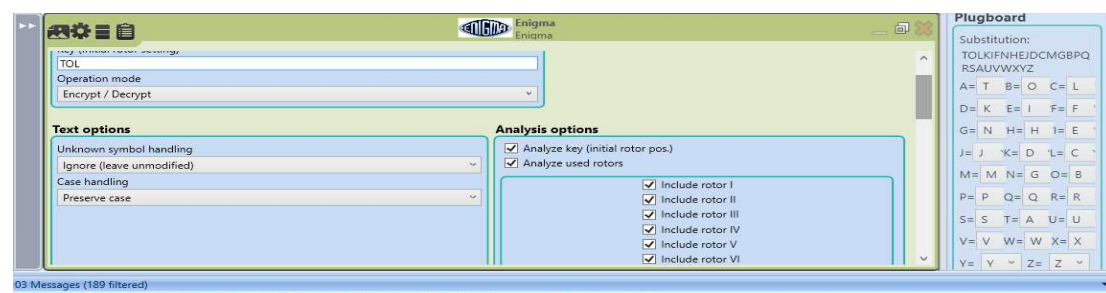
Rotores I,II,III

Inicio: TOL

Reflector: UKW C

Configuración Ringstellung: I I I, Reflector I

Plugboard: A -> T B -> O C -> L D -> K E -> I E -> F G -> N



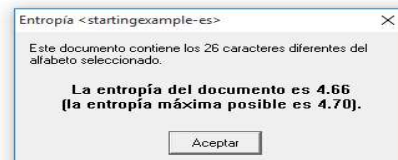
Texto cifrado:

OP WZRSCZ D.S.Y LveokjyVx qmv tbsrkc cz lu bcgnx mobiob ij Ygfzwf. Qk ar ovphcdh zúquwq, mmyai, tgentctrhf, sje onajwq wl ovjcqy z ncwl g edlph, wp qqbnqd nt uoforja fmzw, hclhani p eqteqza, rsu jmht de net kfjmiyic d xmt ntdxt: ows tb rippxsw vhcsh, t bwd joyvunqak ifdwpjhkj. Nkvif fke cdsxoq ackwqtqf, ypjjfobu bcah

yc ylr gn qngf, jvdzqe yd zhlby, jsu jhk jivyhyj ku gxaxiy oxbcmo l neozojwvl, xtesw km dk tqore. Ov dntcgv jz ovkíl n cx olegíxmsg qxeíqbbsos, yvee ft vúcax: hj ouépk ydt eóqdcg, qsm ryjfy, vcm aofnhnf iqlifvxfk bd yttwd x rxbzkr mvnhxnebc q zhvkbsytqmo, apipglyut ku xsjigk ujioagkfvn, d dgectkze v fkralqdw sn nqcuujn zrit veghzgqla r iflwokj; gf rvsysu sub yzlzjtvbbgk y ufq cuosjmc.

- **Entropía:** 4.66. Recordamos que la máxima es 4.70. La mejor alcanzada hasta ahora, esto nos dice que los caracteres están muy bien repartidos.

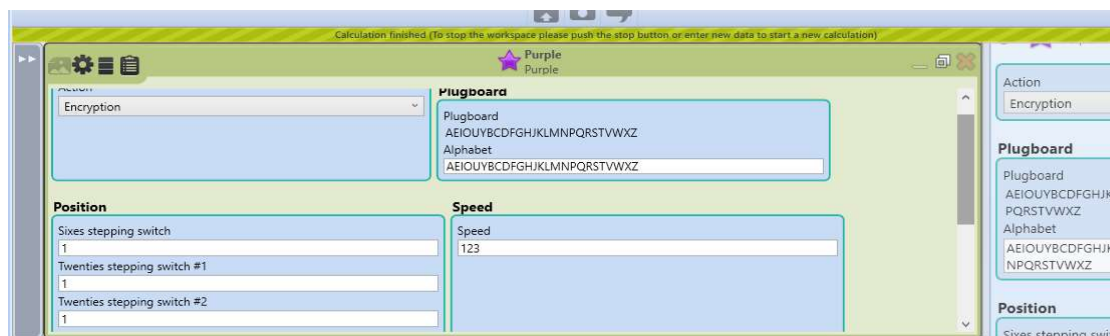
j Ygfzwf. Qk ar ovphcdh zúquwq, mmyai, tgenctgrhf, sje onajwq wl ovjcqy z ncwl g edlph, wp qqbnqjd nt uoforja fmzn vhsah, t bwd joyvunqak ifdwphljkj. ah yz ylr gn qngf, jvdzqe yd zhlby, jsu jhk jivyhyj ku gxaxiy oxbcmo l neozojwvl, xtesw km dk tqore. Ov dntcgv jz c fy, vcm aofnhnf iqlifvxfk bd yttwd x rxbzkr mvnhxnebc q zhvkbsytqmo, apipglyut ku xsjigk ujioagkfvn, d dgectkze v fq cuosjmc.



Respecto a los cuatrigramas la frecuencia es todavía menor, nunca se repiten, esto hace que ante un mensaje más corto, mucho mejor aún menos n-gramas repetidos, siendo un sistema muy robusto para la encriptación y el mejor de los que he usado para este ejercicio.

MÁQUINA PURPLE

Configuración:



Texto codificado:

AK TAKNYT G_H_P GylneedOc iny ejecyci yj ov xyete web_ja id Kughel_Zo am ecybizu r_kote_zodya_vovazxsyji_zih nostaf bo rylepo o anet o tuhjy_ge pinwypa up uqagapu nihu_xumvpi y uxixywo_vyb koxu ev pyo byqlebsi o fey waful_iky ux ecybolu lifvus_o ove gudrofibi depigekoz_Nyv_e aco faevte hupajmu_syjvycne nuxy ar izo ru xuey_tevquty sa dikxy_syz ego zysebli ho jgagfi qypyma i qquvqecji_zenka al iq nycey_Za cuebda ky efk_u e aw mipm_sydo zyk_fbdaci_wake yh c_waw_en v_had sye h_kebi_vuj kiwym_peg besunyw nyhofnakad pa zebudi u pionom ogfasyxar o yvloghfiwug_fxytaccdir le dihsax satqohugoz_a demwejek o qibhuvyz wa kuvbtup cuty taqhdalow i oggikix_aj pehsosf eju yvihzeegyxy a lip qakiwyb_

COMPARACIONES:

Monoalfabetico

Vignere

Enigma

Purple

Entropía

4.09

4.59

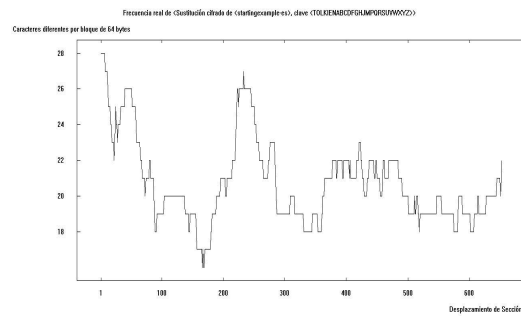
4.66

4.49

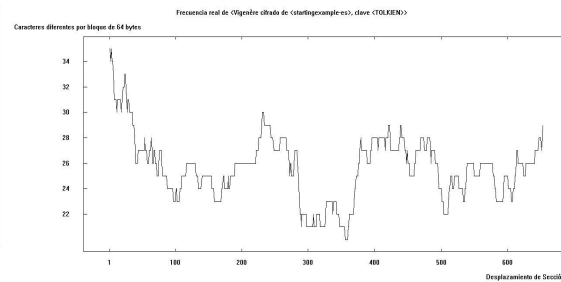
La mejor entropía la obtiene la máquina Enigma, por lo que tiene una mayor variación de letras a la hora de cifrar. Es uno de los factores por la que es mejor que las demás.

Distribucion de frecuencias

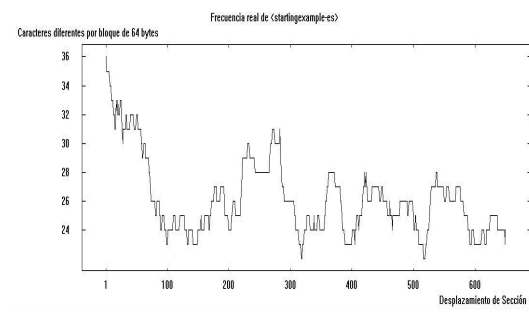
Monoalfabético



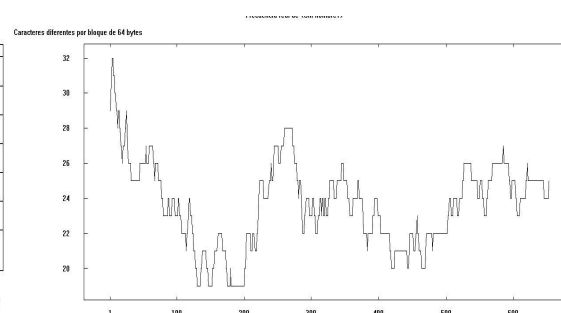
Vignere



Enigma



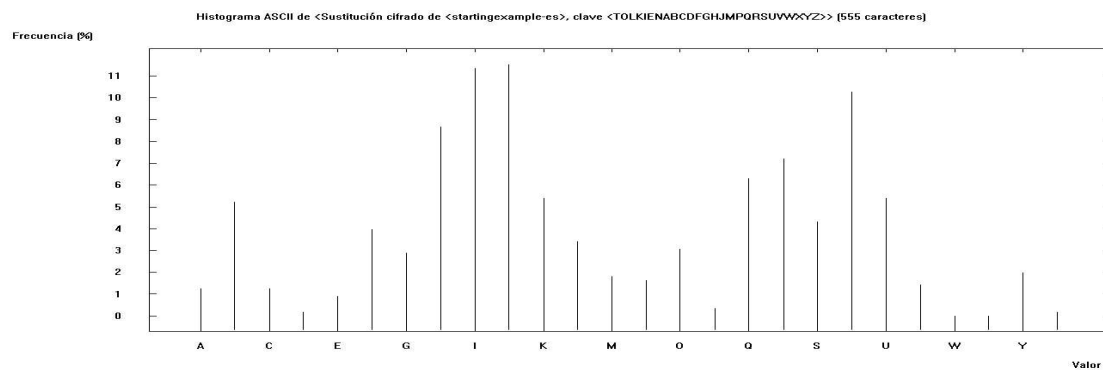
Purple



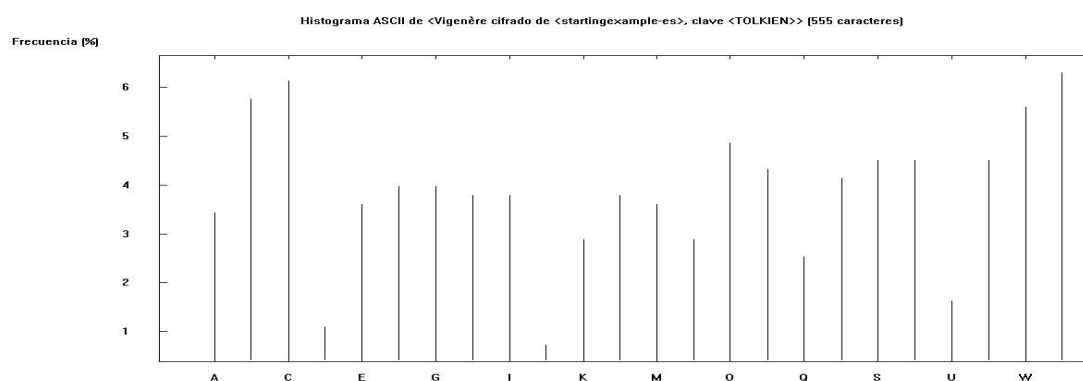
Aquí vemos como las letras más usadas en la permutación del alfabeto, las podemos ver que son las que tiene una mayor frecuencia en el cifrado monoalfabético.

Histograma

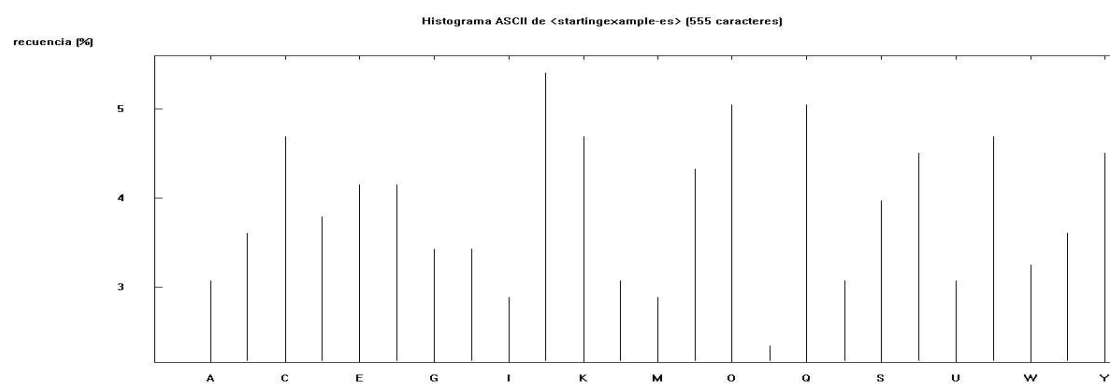
Monoalfabético



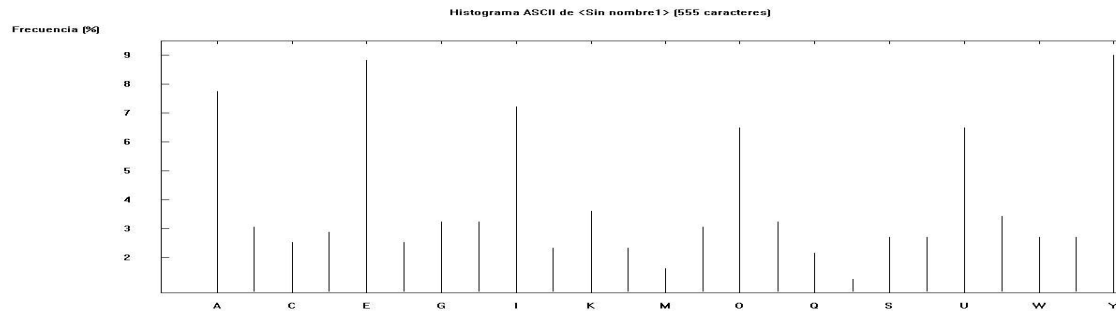
Vignere



Enigma



Purple

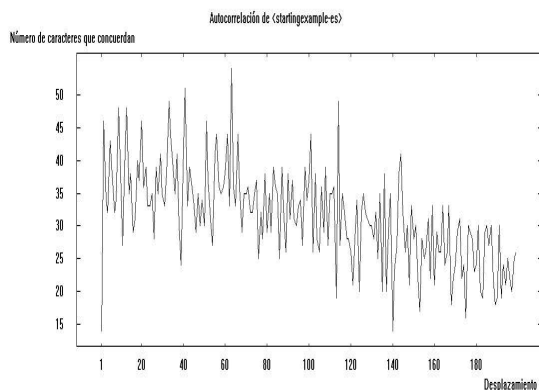


Aquí vemos como la solución monoalfabética tiene un histograma más claro, con unas letras más usadas claramente (I,J,T,U), las cuales las podemos permutar en el alfabeto español a las A,E,R,S [...], ya que simplemente es un desplazamiento de los alfabetos.

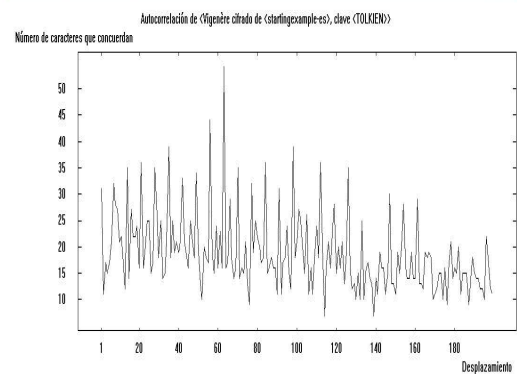
Respecto a la Máquina Enigma, aquí tiene un reparto del alfabeto algo peor que la máquina Purple.

Autocorrelación

Monoalfabético

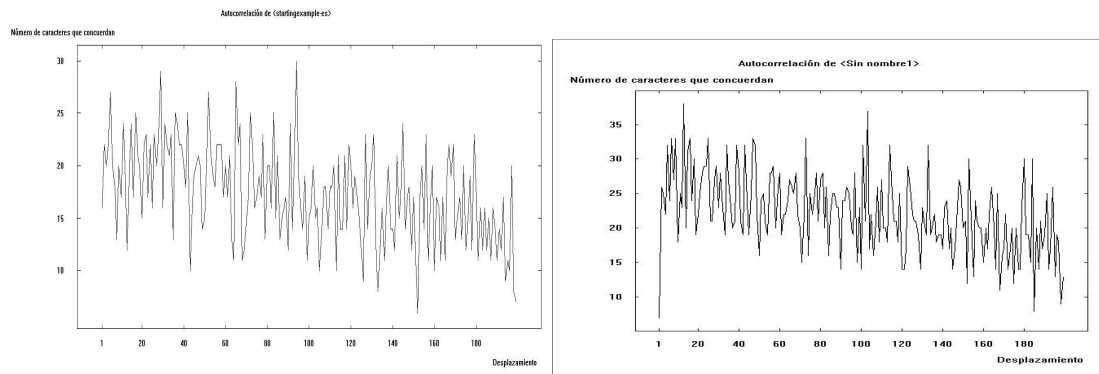


Vignere



Enigma

Purple



Análisis Trigramas

Monoalfabético

Nº	Subcadena	Frecuencia (en %)	Frecuencia
1	IQJ	1.6287	5
2	AJO	1.3029	4
3	CIQ	1.3029	4
4	JOO	1.3029	4
5	LIG	1.3029	4
6	NUC	1.3029	4

Vignere

Nº	Subcadena	Frecuencia (en %)	Frecuencia
1	AXB	0.6515	2
2	CRN	0.6515	2
3	EQT	0.6515	2
4	FTM	0.6515	2
5	GSA	0.6515	2
6	HBL	0.6515	2

Enigma

Purple

Nº	Subcadena	Frecuencia (en %)	Frecuencia	Nº	Subcadena	Frecuencia (en %)	Frecuencia
1	OKJ	0.6515	2	1	ECY	0.9772	3
2	ACK	0.3257	1	2	BDA	0.6515	2
3	AGK	0.3257	1	3	CYB	0.6515	2
4	AJW	0.3257	1	4	EJE	0.6515	2
5	ALQ	0.3257	1	5	IWY	0.6515	2
6	ANI	0.3257	1				

Vemos como la mejor es la Enigma, ya que solo repite una vez Trigramas, mientras que en el caso del cifrado Monoalfabético llego hasta 5 repeticiones.

Cuatrigramas

Monoalfabético

Nº	Subcadena	Frecuencia (en %)	Frecuencia
1	AJOO	1.8018	4
2	CIQJ	1.8018	4
3	JOOB	1.8018	4
4	NUCI	1.8018	4
5	O OBS	1.8018	4
6	TNUC	1.8018	4
7	UCIQ	1.8018	4

Vignere

Nº	Subcadena	Frecuencia (en %)	Frecuencia
1	AXBL	0.9009	2
2	FTMV	0.9009	2
3	STPN	0.9009	2
4	TMVB	0.9009	2
5	TUFT	0.9009	2
6	UFTM	0.9009	2
7	ABTT	0.4505	1
8	ACML	0.4505	1

Enigma

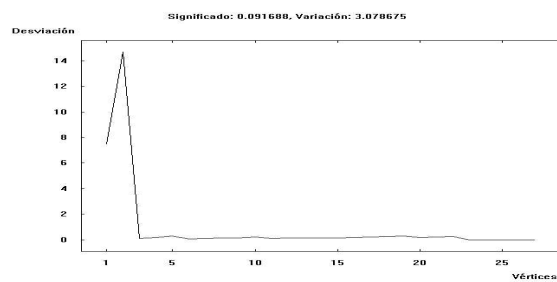
Purple

Nº	Subcadena	Frecuencia (en %)	Frecuencia	Nº	Subcadena	Frecuencia (en %)	Frecuencia
1	ACKW	0.4505	1	1	ECYB	0.9009	2
2	AGKF	0.4505	1	2	KIWI	0.9009	2
3	AJWQ	0.4505	1	3	ACDI	0.4505	1
4	ALQD	0.4505	1	4	AEVT	0.4505	1
5	AOFN	0.4505	1	5	AFUL	0.4505	1
				6	AGAP	0.4505	1

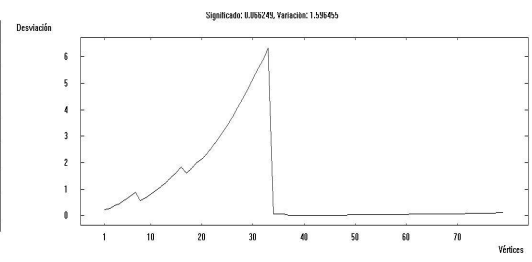
No se repiten cuatrigramas en una máquina Enigma en un mensaje no muy largo, alrededor de 1000 palabras.

VITANY - Análisis de aleatoriedad

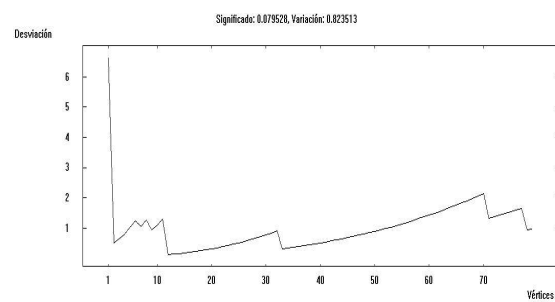
Monoalfabético



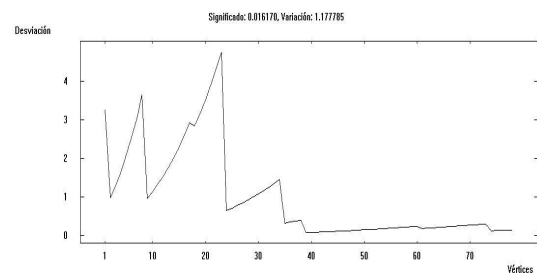
Vignere



Enigma

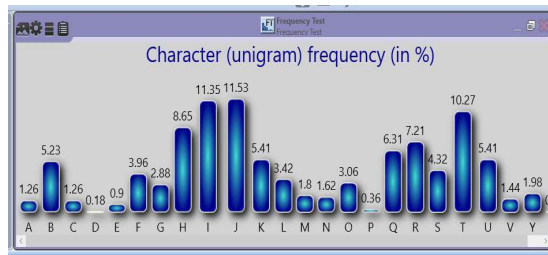


Purple

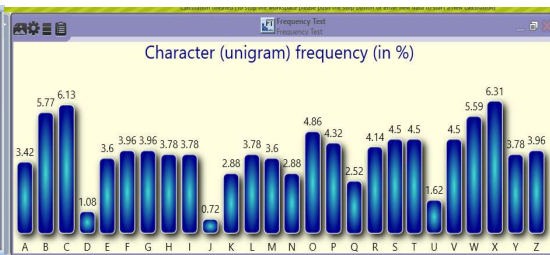


- Test Frecuencias

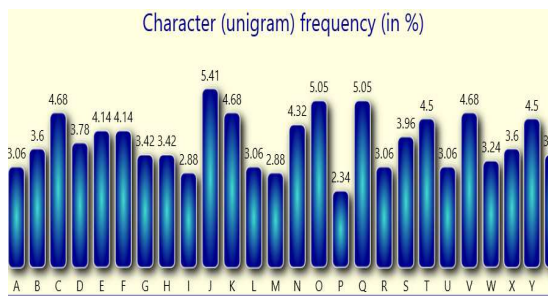
Monoalfabético



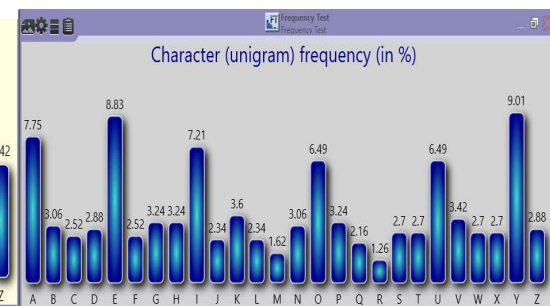
Vignere



Enigma



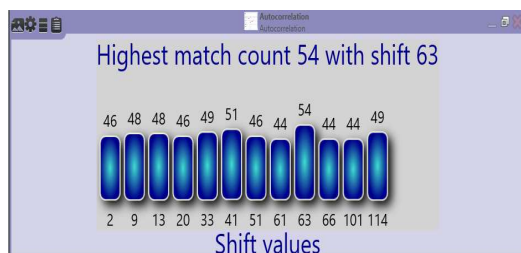
Purple



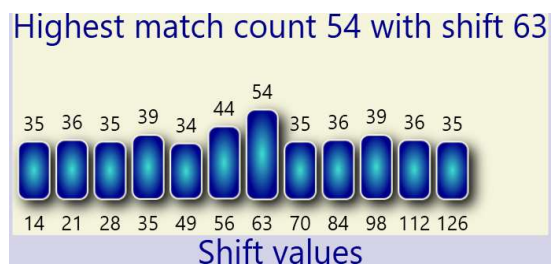
Igual que antes, la que mejor distribuye las frecuencias es la máquina Enigma, mientras que el cifrado monoalfabético podemos ver el desplazamiento del alfabeto, I podría ser la A ...etc.

Autocorrelación

Monoalfabético

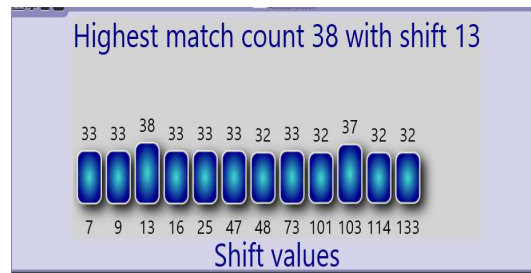
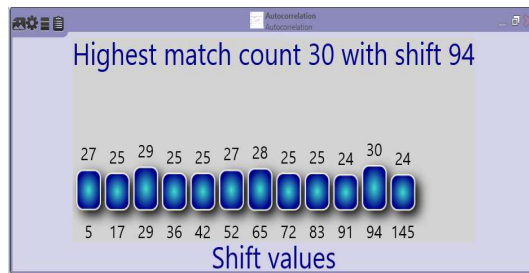


Vignere



Enigma

Purple



Vemos como la que tiene una mejor autocorrelación y un mejor "reparto" en el alfabeto es la máquina Enigma, la cual apenas repite n-gramas en un mensaje.

CONCLUSIÓN:

El más fuerte sería ENIGMA, seguido de PURPLE, ya que ambos distribuyen muy bien la frecuencias y la autocorrelación en el abecedario y apenas tienes repeticiones. Después iría el cifrado de Vignere, que sería más débil debido a que si se encuentra la clave se encuentra el descifrado, y por último el Monoalfabético, que simplemente es un desplazamiento de letras en el abecedario, y podemos sustituir la A -> clave X ...

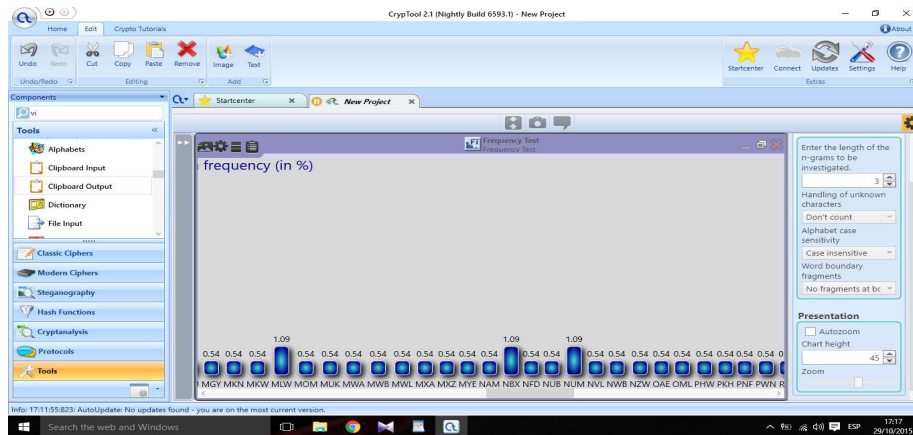
Todo esto, además de que tiene una mejor Entropía, podemos concluir que la máquina ENIGMA es la mejor de todas para cifrar, cifrando aún mejor mensajes no demasiado largos en los que no se vuelva al estado inicial de los rotores, es decir, no se de la vuelta en los 3 rotores al abecedario.

Además podemos ver como por ejemplo además de la entropía, la máquina enigma es la que tiene una autocorrelación más repartida a lo largo del abecedario.

9. Realizar un análisis al "Texto cifrado que venció a Poe" (Cifrado Poe_ejemplo_3), usando esta herramienta.

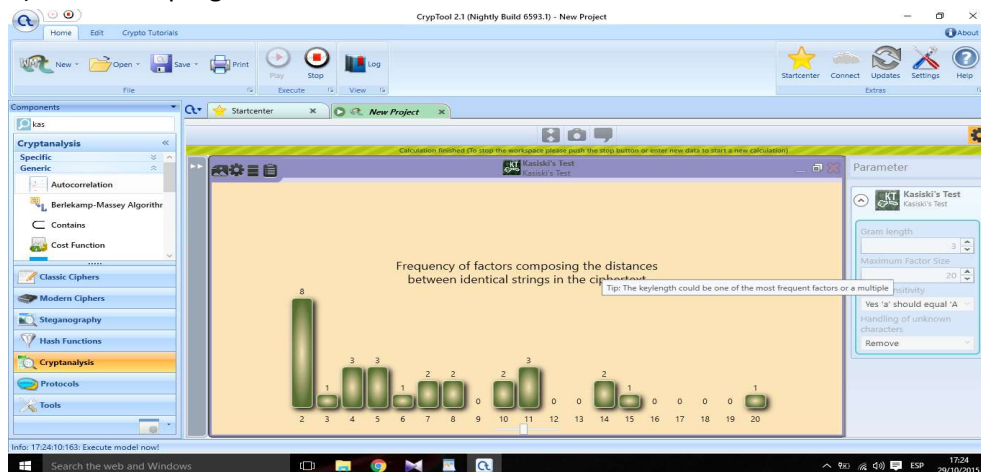
- a) Hacer un Análisis de Trigramas repetidos con CrypTool y determinar cuáles son.
- b) Calcular el periodo mediante el método de Kasiski aplicado al apartado anterior.
- c) Modificar el periodo obtenido por la autocorrelación con los datos de b).
- d) Obtener resultados parciales para intentar arreglar el problema grave anunciado en el texto cifrado.

Para el análisis de trigramas usamos un análisis de frecuencias y seleccionamos como 3 el número de ngramas. Vemos que los tres más repetidos son: (MLW,NBX,NUM)



Vemos que todos los demás trigramas están bastante bien distribuidos, y estos 3 solo aparecen un poco más que los demás, sólo 0.5% en términos de frecuencia.

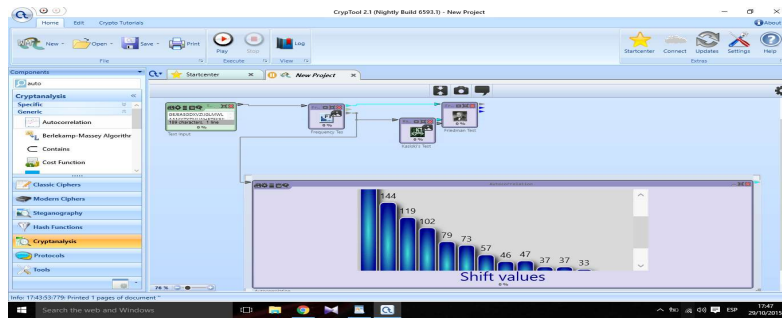
b) Análisis Criptográfico -> Test Kasiski



Vemos que el trigrma que más veces se repite es el primero, que se repite hasta 8 veces.

c) Autocorrelación:

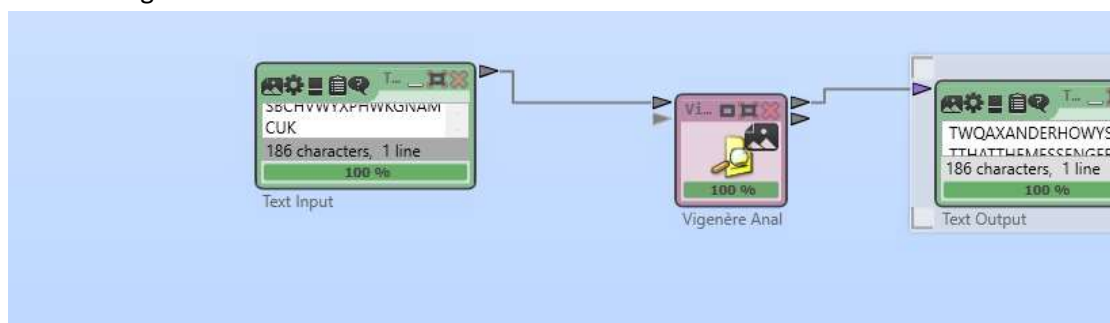
AAM:1:0,00543478260869565



AAN:1:0,00543478260869565
 AEG:1:0,00543478260869565
 AGH:1:0,00543478260869565
 AHU:1:0,00543478260869565
 AIV:1:0,00543478260869565
 ALP:1:0,00543478260869565
 AMC:1:0,00543478260869565
 AMX:1:0,00543478260869565
 ANU:1:0,00543478260869565
 ASG:1:0,00543478260869565
 ATG:1:0,00543478260869565
 BAI:1:0,00543478260869565
 BCH:1:0,00543478260869565
 BMX:1:0,00543478260869565
 BRA:1:0,00543478260869565
 BXM:1:0,0054347826...

d) Obtener resultados parciales

He usado el cifrado de Vignere, que da resultados parciales debido a que el mensaje contiene algunos errores en el cifrado:



Texto llano generado:

TWQ AXANDER HOW Y SIT THAT THE MESSENGER ARRIVES HERE AT THE SACE TIME WITH THE SATURGAY COURIER AND OTHER SATUZDA OPATERS WHEN AVCORDIDG TO THE CATEITIS PUBLISHRD THREE DAY SPREVIOUSIS THE FAULT WITG YOU ORTGE POSS MASTYRS

El texto es una carta a un director del periódico "The Messenger". El problema está en que

la segunda letra de Alenxand(e)r no está, y por eso falla el código. El descifrado sería así:

TO ALEXANDER HOW IS IT, THAT, THE MESSENGER ARRIVES HERE AT THE SAME TIME WITH
THE SATURDAY COURIER AND OTHER SATURDAY PAPERS WHEN ACCORDING TO THE DATE
IT IS PUBLISHED THREE DAYS PREVIOUS IS THE FAULT WITH YOU OR THE POSTMASTERS?

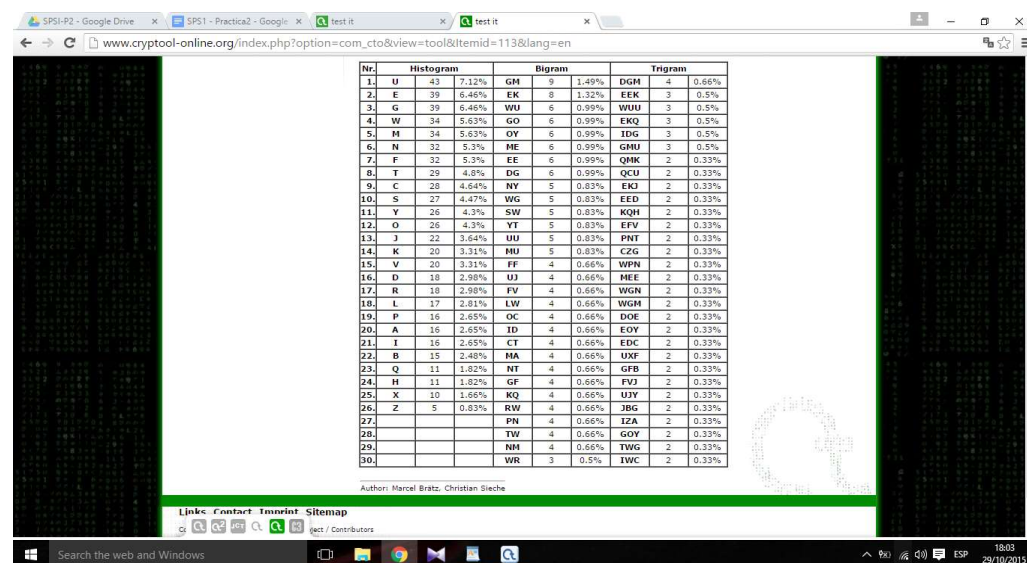
10. Descifrar el texto dado en el “Cifrado ejemplo_4”. Para ello:

a) Determinar el tipo de cifrado aplicado. Determinar información sobre entropía, N-gramas, Autocorrelación, periodicidad, ... y confirmar con toda esta información el tipo de cifrado.

b) Descifrarlo con la herramienta de análisis adecuada de CryptTool.

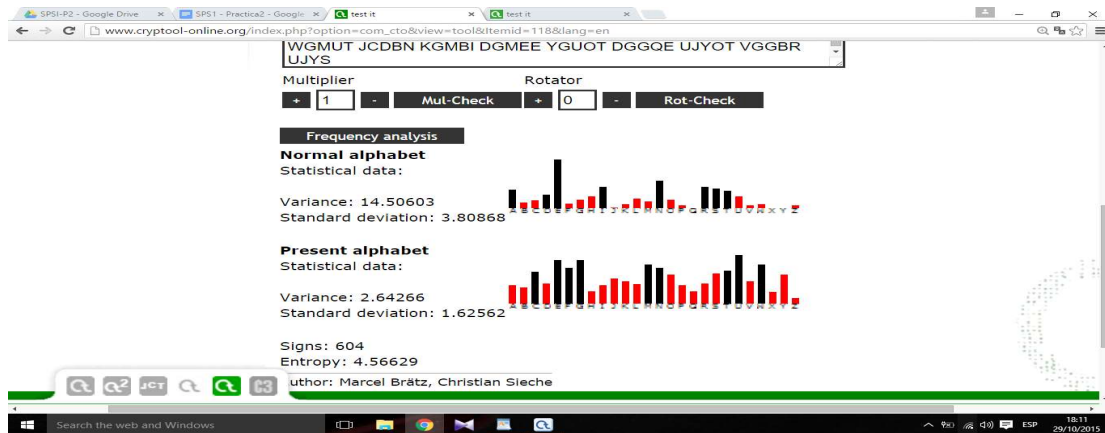
He usado en algunos momentos la herramienta de cryptool Online.

Análisis de trigramas: vemos que las letras para 1 1-grama las más usadas son las U,E,G. Aún así vemos que hasta la letra L, se repiten mucho las letras. En cambio para bigramas tenemos un reparto más igualitario, donde las más usadas son GM,EK,WU. Tigramas están aún más repartidos, donde apenas se repiten, tenemos los más usados DGM,EEK,WUU.



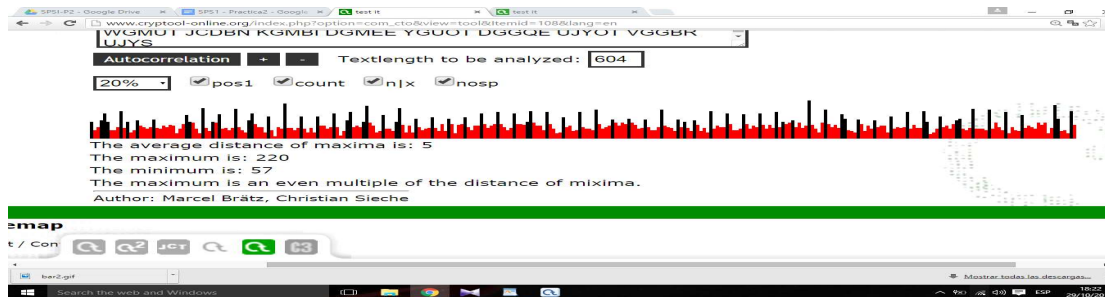
Nr.	Histogram	Bigram	Trigram
1.	U 43 7.12%	GM 3 1.49%	DGM 4 0.66%
2.	E 39 6.46%	EK 8 1.32%	EEK 3 0.5%
3.	G 39 6.46%	WU 6 0.99%	WUU 3 0.5%
4.	W 34 5.63%	GO 6 0.99%	EKQ 3 0.5%
5.	H 34 5.63%	OY 6 0.99%	IDG 3 0.5%
6.	N 32 5.3%	ME 6 0.99%	GMU 3 0.5%
7.	F 32 5.3%	EE 6 0.99%	QMK 2 0.33%
8.	T 29 4.6%	DG 6 0.99%	QCU 2 0.33%
9.	C 28 4.64%	NY 5 0.83%	EKJ 2 0.33%
10.	S 27 4.47%	WG 5 0.83%	EED 2 0.33%
11.	Y 26 4.3%	SW 5 0.83%	KQH 2 0.33%
12.	O 26 4.3%	YT 5 0.83%	EFV 2 0.33%
13.	J 22 3.64%	UU 5 0.83%	PNT 2 0.33%
14.	K 20 3.31%	MU 5 0.83%	CZG 2 0.33%
15.	V 20 3.31%	FF 4 0.66%	WPN 2 0.33%
16.	D 18 2.98%	UJ 4 0.66%	HEE 2 0.33%
17.	R 18 2.98%	FV 4 0.66%	WGN 2 0.33%
18.	L 17 2.81%	LW 4 0.66%	WGM 2 0.33%
19.	P 16 2.65%	OC 4 0.66%	DOE 2 0.33%
20.	A 16 2.65%	ID 4 0.66%	EOY 2 0.33%
21.	I 16 2.65%	CT 4 0.66%	EDC 2 0.33%
22.	B 15 2.48%	HA 4 0.66%	UXF 2 0.33%
23.	Q 11 1.82%	NT 4 0.66%	GFB 2 0.33%
24.	H 11 1.82%	GF 4 0.66%	FVJ 2 0.33%
25.	X 10 1.66%	KQ 4 0.66%	UJY 2 0.33%
26.	Z 5 0.83%	RW 4 0.66%	JBG 2 0.33%
27.		PN 4 0.66%	IZA 2 0.33%
28.		TW 4 0.66%	GOY 2 0.33%
29.		NM 4 0.66%	TWG 2 0.33%
30.		WR 3 0.5%	IWC 2 0.33%

Periodicidad:



Aquí vemos que la **Entropía** es muy alta, 4.56, recordemos que la máxima es 4.7 en cryptool, está medianamente bien repartido el uso de letras. Aún así con el gráfico podemos hacer una pequeña correlación del alfabeto, cambiando las letras de las ternas más usadas {A,D,E,I,N,R,S,T} → {C,E,F,G,M,N,T,U,W}

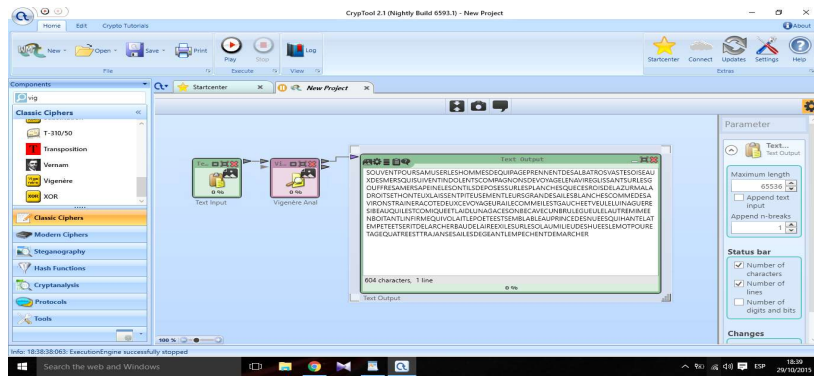
Autocorrelación:



Vemos que hay un período mayormente claro, onda que sube y baja siempre. Tiene características propias de un texto de Vignere. Creo que es un texto cifrado con Vignere, por lo que podemos probar:

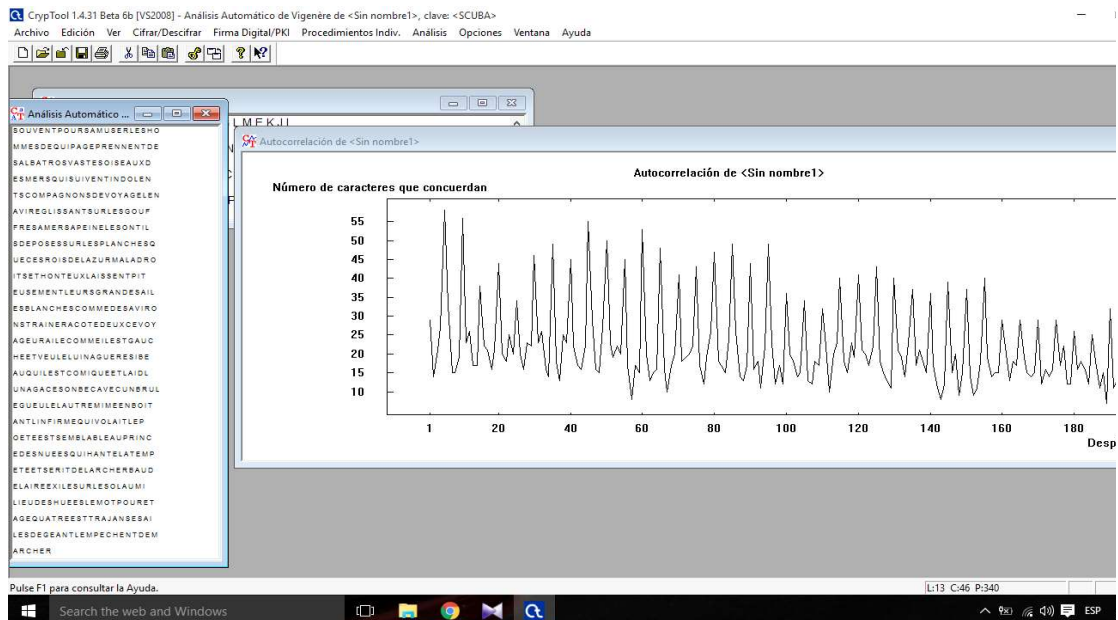
Texto obtenido en **francés**:

SOUVENTPOURSAMUSERLESHOMMESDEQUIPAGEPRENNENTDESALBATROSVASTESOISEAU
 XDESMERSQUISUIVENTINDOLENTSCOMPAGNONSDEVOYAGELENAVIREGLISSANTSURLESGO
 UFFRESAMERSAPEINELESONTILSDEPOSESSURLESPANCHESQUECESROISDELAZURMALADRO
 ITSETHONTEUXLAISSENTPITEUSEMENTLEURSGRANDESAILESBLANCHESCOMMEDESAVIRONS
 TRAINERACOTEDEUXCEVOYAGEURAILCOMMEILESTGAUCHEETVEULELUINAGUERESIBEAU
 QUILESTCOMIQUEETLAIDLUNAGACESONBECAVECUNBRULEGUEULELAUTREMIMEENBOITAN
 TLINFIRMEQUIVOLAITLEPOETEESTSEMBLABLEAUPRINCEDESNUESQUIHANTELATEMPETEET
 SERITDELARCHERBAUDELAIREEXILESURLESOLAUMILIEUDES HUEESLE MOTPOURETAGEQUAT
 REESTTRAJANSESAILSEDEGEANTLEMPECHENTDEMARCHER



SOUVENT **POUR** SAMUSERLES **HOMMES** D **EQUIPAGE** PRENNENT DES ALBATROS
VASTESOISE **AUX** DES MERSQUI SUIVENTIN DOLENTS COMPAGNONS DE **VOYAGE** LE
NAVIREGLISSANT **SUR** LES GOUFFRES AMERSAPEINELES ONTILS DE POSESSURLES PLANCHES
QUE CES ROIS DELAZURMALADROITS ET HONTEUXLAISSENTPITEUSEMENTLEURS GRANDE
SAILES **BLANCHES** COMME DE SAVIRONSTRAINERA COTE **DEUX** CE **VOYAGE** URAILE COMME
IL **EST** GAUCHE ET VEU LE LUINA GUERE SI BEAU QUILEST COMIQUE ET LAID LUNA
GACESONBECAVECUNBRULEGUEULE LAUTRE MIMÉEN BOITANT LIN FIRME QUIVOLAITLE
POETEEST SEMBLA BLEAU PRINCE DES NUE ESQUIHANTELA TEMPETEET SERITDEL ARCHER
BAU DE LAIRE EXILE SUR LES OLAUMILIEU DES HUEESLEMOT POUR ETAGE QUATRE EST
TRAJAN SESAILES DE GEANTLEMPECHENT DE MARCHER

Probamos con Cryptool 1 para obtener además la clave, que en este caso es **SCUBA**:



11. Resolver el triple reto de Mystery Twister C3 contenido en el fichero mtc3-wacker-01-classicalciphers3-en usando la herramienta CrypTool y dando las 3 palabras código pedidas.

Fase 1: César

Donx dlqd kdqndod, orsxvvd nllwrv vhlvrr.

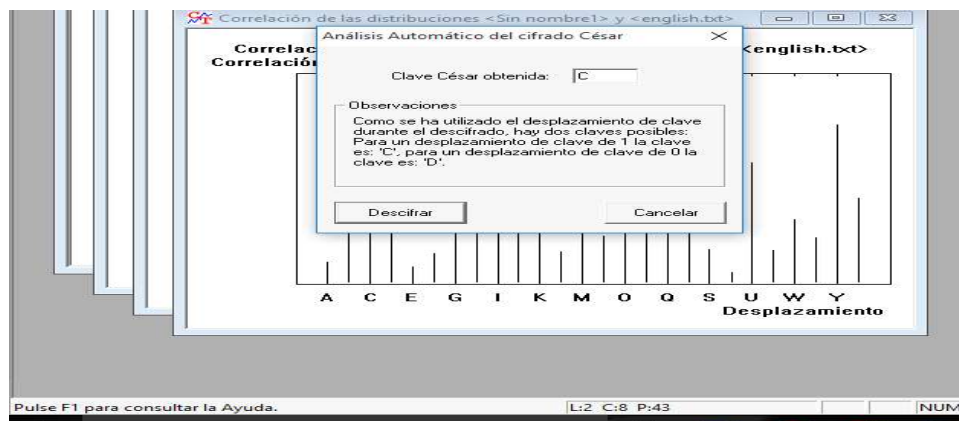
Me salé un texto en finés, que habla de los problemas de caries el día de acción de gracias.

Finés: Alku aina hankala, lopussa kiitos
seisoo.

Español: El comienzo de los problemas al final de todo el trabajo duro.

Clave C, tercera palabra del código **hankala**

Codeword: hankala



Fase 2: Cifrado por sustitución

He hecho un cifrado por sustitución del resultado del mensaje 1, descifrado.

TIME THAT hTAMTIT lopEsST MHHTos seHsoo

Codeword: TIME

Fase 3: Cifrado desconocido

Está cifrado en Navajo, lo he descubierto buscando las palabras separadas.

He usado este especie de diccionario:

<http://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/n/navajo-code-talker-dictionary.html>

Está hecho, el código es navajo.

UT-ZHA!, CHA-GEE YIL-TAS SEIS TSAH WOL-LA-CHEE A-KEH-DI-GLINI TSE-NILL

Esta hecho, el "código es aguja hormiga victor hacha
N A V A

AH-YA-TSINNE NE-AHS-JAH

mandíbula búho"

j o

La traducción normal, es :

Está hecho, el código es NAVAJO, ya que debajo dice el sentido literal de las letras, siendo aguja la letra N (needle), hormiga A (ANT), hacha A (axe), mandíbula J (jaw) y búho O (owl).

Codeword: NAVAJO

12. Resolver el reto de Mystery Twister C3 contenido en el fichero mtc3-simon- 02-adfgvx-en cifrado con el algoritmo ADFGVX, usando también esta herramienta.

ADGG AADG FDFA AVFD DAAV GDFF DXFG
AFAA DDDF GFGD FFAG VDDF AFFG AADG
AAAG AAGD FFDA GFAA GGAG DGAA AAAD
GGAD DAAA GAFA GGGA ADAD FAAA

No he conseguido descifrarlo, he intentado usar la clave ENI, en el orden 1 - 2 -3 que es EIN:

