



UAI

Universidad Abierta Interamericana

Facultad de Tecnología Informática

Seguridad Informática

Trabajo Práctico Nº 02: Encriptado Clásico

Grupo Rojo

Alumnos Otto Gonzalez, Franco Fazzito, Bárbara Covarrubias,
Franco Fazzito, Malena Aguillon, Franco Balich

Profesor **Marcelo Semería**

Fecha **22/09/2022**

*OK pasar a la
nueva actividad*

SEGURIDAD INFORMATICA

TP #2 Criptografía Clásica

PARTE A : Cryptool – Propiedades de los Cifrados

Tarea 1-1

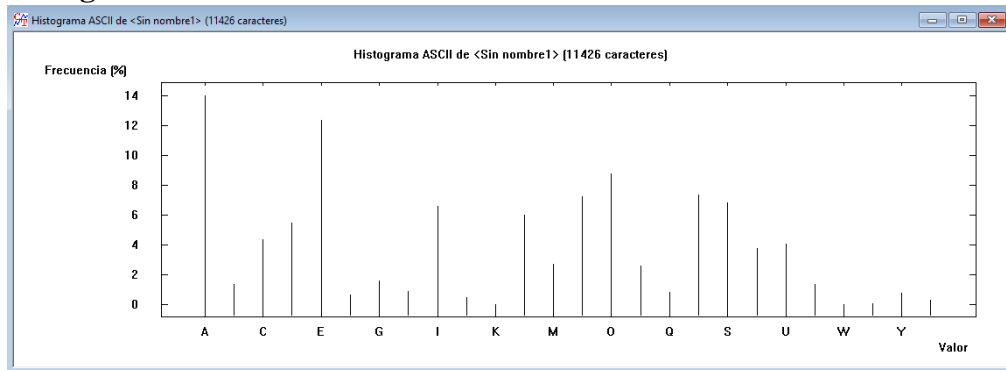
Escriba o copie tres textos extensos (10.000 letras o mas) en español . Los textos deben ser de distinto tipo (Ej: Novela Histórica, Diario Clarin, Manual de plomería). Mediante **Cryptool** encuentre el listado de:

- La frecuencia de letras
- La frecuencia de diagramas (conjunto de dos letras)
- La frecuencia de triagramas (conjuntos de tres letras)

¿Dependen los resultados obtenidos del tipo de texto? Explique

Texto 1

Histograma texto 1



Lista de N-Gramas de Sin nombre1

Selección:	Nº	Secuencia de ...	Frecuencia en...	Frecuencia
<input checked="" type="radio"/> Histograma (25)	1	A	14.0119	1601
<input type="radio"/> Digrama (259)	2	E	12.3490	1411
<input type="radio"/> Trigrama (1178)	3	O	8.7520	1000
<input type="radio"/> 4 -grama (1859)	4	R	7.3079	835
Mostrar los 25	5	N	7.2029	823
N-gramas más comunes (valores permitidos: 1-5000)	6	S	6.8090	778
Opciones de Texto	7	I	6.5815	752
	8	L	5.9776	683
	9	D	5.4612	624
	10	C	4.3147	493
	11	U	4.0259	460
	12	T	3.7633	430
	13	M	2.7044	309
	14	P	2.5818	295
	15	G	1.5666	179
	16	V	1.3478	154
	17	B	1.3215	151
	18	H	0.8664	99
	19	Q	0.8314	95
	20	Y	0.7527	86
	21	F	0.6214	71
	22	J	0.4901	56
	23	Z	0.2888	33
	24	X	0.0613	7
	25	W	0.0088	1

Calcular lista

Guardar lista

Cerrar

Diagrama texto 1

Lista de N-Gramas de Sin nombre1

Selección

☐ Histograma (25)

☒ Digrama (259)

☐ Trigrama (1178)

☐ 4 -grama (1859)

Mostrar los 25

N-gramas más comunes (valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	DE	3.4312	305
2	AR	2.3850	212
3	LA	2.1375	190
4	EN	2.1150	188
5	EL	1.9575	174
6	ES	1.9012	169
7	ER	1.8337	163
8	NA	1.7437	155
9	SA	1.7437	155
10	AN	1.7100	152
11	UE	1.6425	146
12	OS	1.6087	143
13	RA	1.6087	143
14	NT	1.5412	137
15	LD	1.5300	136
16	AD	1.4962	133
17	DO	1.3950	124
18	ON	1.3500	120
19	OR	1.2712	113
20	AS	1.2487	111
21	CA	1.2375	110
22	RE	1.2375	110
23	CI	1.2262	109
24	IA	1.2037	107
25	TI	1.1025	98

Trigrama Texto 1

Lista de N-Gramas de Sin nombre1

Selección

☐ Histograma (25)

☐ Digrama (259)

☒ Trigrama (1178)

☐ 4 -grama (1859)

Mostrar los 25

N-gramas más comunes (valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	QUE	1.1239	74
2	SAN	1.0176	67
3	LOS	0.9417	62
4	ANT	0.8961	59
5	ENT	0.7746	51
6	ASA	0.7594	50
7	NTI	0.7442	49
8	ICA	0.7139	47
9	ADO	0.6835	45
10	IAG	0.6835	45
11	TIA	0.6835	45
12	AGO	0.6531	43
13	NTE	0.6227	41
14	SAR	0.6227	41
15	CAR	0.6075	40
16	CON	0.6075	40
17	EST	0.6075	40
18	NCI	0.6075	40
19	DEL	0.5772	38
20	PER	0.5772	38
21	NAS	0.5620	37
22	RIO	0.5468	36
23	ARI	0.5164	34
24	DES	0.4708	31
25	CIA	0.4557	30

Explicación analizada:

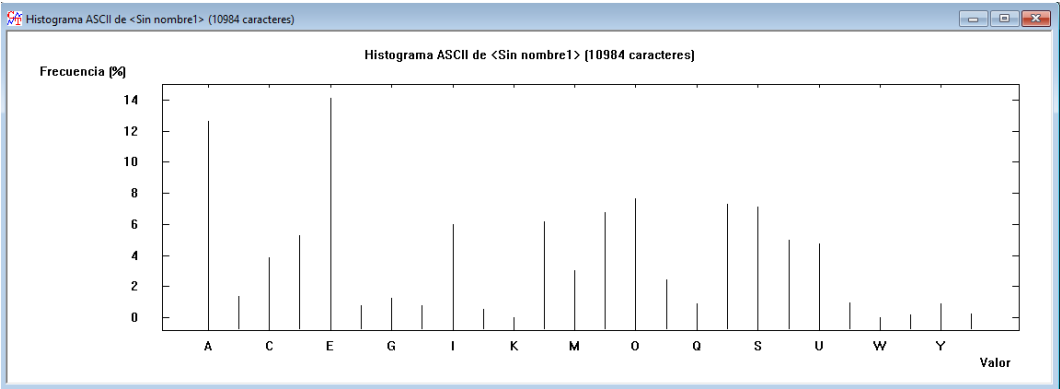
En este contexto, se pueden observar que las letras más repetidas en el texto 1 son la A, E, y O, luego en menor medida la R, la N y la S. Las letras menos frecuentes son la J, W, Z y la X.

A partir de los datos anteriores:

- Las consonantes más frecuentes son: R, S, N, L, D, C (aparecen con una frecuencia de un 37%)
- Las vocales ocuparán alrededor del 44% del texto.
- Las seis letras menos frecuentes son: Z, J, Ñ, X, K, W (sumadas tienen una frecuencia que apenas supera el 1%).
- La A y la E son identificables fácilmente dado su porcentaje de aparición.

Texto 2

Histograma Texto 2



Lista de N-Gramas de Sin nombre1

Selección:

☒ Histograma (25)

☐ Digrama (249)

☐ Trigramas (1101)

☐ 4 -grama (1741)

Mostrar los 25

N-gramas más comunes (valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	E	14.1296	1552
2	A	12.6457	1389
3	O	7.6566	841
4	R	7.2833	800
5	S	7.1103	781
6	N	6.7917	746
7	L	6.1544	676
8	I	6.0087	660
9	D	5.3077	583
10	T	4.9800	547
11	U	4.7615	523
12	C	3.8511	423
13	M	3.0499	335
14	P	2.4672	271
15	B	1.3474	148
16	G	1.2655	139
17	V	0.9468	104
18	Q	0.8831	97
19	Y	0.8831	97
20	F	0.7647	84
21	H	0.7465	82
22	J	0.5371	59
23	Z	0.2185	24
24	X	0.1821	20
25	W	0.0273	3

Diagrama Texto 2

Lista de N-Gramas de Sin nombre1

Selección				
<input type="radio"/> Histograma (25)	Nº	Secuencia de ...	Frecuencia en...	Frecuencia
<input checked="" type="radio"/> Digrama (249)	1	DE	3.1394	265
<input type="radio"/> Trigrama (1101)	2	EN	2.8196	238
<input type="radio"/> 4 -grama (1741)	3	ES	2.5352	214
Mostrar los 25	4	ER	2.1088	178
N-gramas más comunes	5	EL	2.0732	175
(valores permitidos: 1-5000)	6	LA	2.0258	171
Opciones de Texto	7	RA	2.0140	170
Calcular lista	8	UE	1.8126	153
Guardar lista	9	RE	1.6941	143
Cerrar	10	NT	1.6586	140
	11	TE	1.5638	132
	12	AR	1.5046	127
	13	ON	1.4572	123
	14	TA	1.4572	123
	15	AL	1.3861	117
	16	ST	1.3506	114
	17	AN	1.3387	113
	18	DO	1.3150	111
	19	SE	1.1965	101
	20	AD	1.1728	99
	21	CI	1.1728	99
	22	OS	1.1728	99
	23	QU	1.1492	97
	24	DA	1.1018	93
	25	UN	1.0781	91

Trigrama texto 2

Lista de N-Gramas de Sin nombre1

Selección				
<input type="radio"/> Histograma (25)	Nº	Secuencia de ...	Frecuencia en...	Frecuencia
<input type="radio"/> Digrama (249)	1	ENT	1.3441	83
<input checked="" type="radio"/> Trigrama (1101)	2	QUE	1.3441	83
<input type="radio"/> 4 -grama (1741)	3	NTE	1.0950	67
Mostrar los 25	4	EST	0.9879	61
N-gramas más comunes	5	TRA	0.8421	52
(valores permitidos: 1-5000)	6	CON	0.7935	49
Opciones de Texto	7	STA	0.7611	47
Calcular lista	8	IEN	0.6964	43
Guardar lista	9	IST	0.6640	41
Cerrar	10	DEL	0.5992	37
	11	PAR	0.5830	36
	12	IDA	0.5668	35
	13	ANT	0.5506	34
	14	PRO	0.5506	34
	15	ADO	0.5344	33
	16	LOS	0.5344	33
	17	RES	0.5344	33
	18	ERT	0.5182	32
	19	ICA	0.5020	31
	20	PER	0.5020	31
	21	DAD	0.4696	29
	22	RAN	0.4696	29
	23	CIA	0.4534	28
	24	UER	0.4534	28
	25	ERA	0.4372	27

Observamos que las letras que más se repiten en el texto 2 son la E, A y O, luego en menor medida la R, la S, N y la L. Las letras menos frecuentes son la J, W, Z y la X.

Explicación del análisis:

A partir de los datos anteriores, se puede decir que:

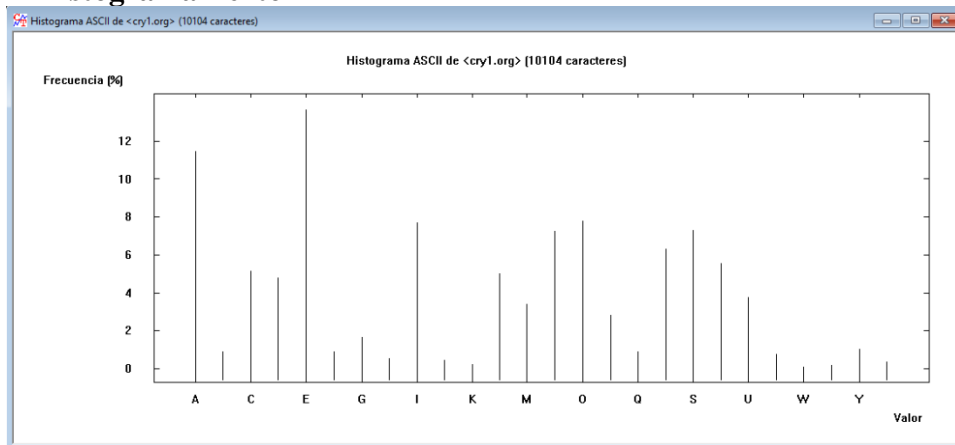
- Las consonantes más frecuentes son: R, N, S, L, D, T (aparecen con una frecuencia aprox un 30%)
- La E, la A y O son identificables fácilmente dado su porcentaje de aparición.
- Las vocales ocuparán alrededor del 42% del texto.
- Las seis letras menos frecuentes son: J, Z, X, K, W (sumadas tienen una frecuencia que apenas supera el 1,5%)

El diagrama DE en ambos textos es el más frecuente, obviamente son palabras del alfabeto español. En ambos textos el trigramma QUE es el que más frecuencia tienen.

Texto 3

Se usó un extracto de un artículo sobre aplicaciones de la inteligencia artificial.

Histograma Texto 2



Lista de N-Gramas de startingexample-es

Selección

☒ Histograma (26)

☐ Digrama (267)

☐ Trigramma (1001)

☐ 4 -grama (1394)

Mostrar los 25

N-gramas más comunes (valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	E	13.8982	1122
2	A	10.9501	884
3	O	7.8905	637
4	I	7.7666	627
5	N	7.4941	605
6	S	7.2340	584
7	R	6.4164	518
8	T	5.6856	459
9	C	5.2521	424
10	L	4.9672	401
11	D	4.7566	384
12	U	3.7285	301
13	M	3.2578	263
14	P	2.8366	229
15	G	1.6351	132
16	Y	1.0157	82
17	B	0.9042	73
18	F	0.9042	73
19	Q	0.9042	73
20	V	0.7432	60
21	H	0.4831	39
22	J	0.4212	34
23	Z	0.3840	31
24	K	0.1982	16
25	X	0.1734	14

Diagrama Texto 3

Lista de N-Gramas de startingexample-es

Selección

☐ Histograma (26)

☒ Digrama (267)

☐ Trigrama (1001)

☐ 4 -grama (1394)

Mostrar los

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	EN	3.6207	231
2	DE	3.1505	201
3	ES	2.7586	176
4	TE	2.3041	147
5	NT	2.2414	143
6	AR	2.1317	136
7	CI	2.0376	130
8	OS	1.9592	125
9	CO	1.8339	117
10	ON	1.6928	108
11	ER	1.6771	107
12	RE	1.6614	106
13	RA	1.4577	93
14	IN	1.3950	89
15	EL	1.3793	88
16	TA	1.3480	86
17	AL	1.3009	83
18	TI	1.2853	82
19	UE	1.2853	82
20	OR	1.2382	79
21	AS	1.1912	76
22	IA	1.1912	76
23	DO	1.1599	74
24	LA	1.1442	73
25	QU	1.1442	73

Trigrama Texto 3

Lista de N-Gramas de startingexample-es

Selección

☐ Histograma (26)

☐ Digrama (267)

☒ Trigrama (1001)

☐ 4 -grama (1394)

Mostrar los

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	NTE	1.8929	93
2	CON	1.3841	68
3	CIA	1.3027	64
4	ENT	1.2416	61
5	QUE	1.0788	53
6	TEN	0.9974	49
7	NCI	0.9770	48
8	ENC	0.8752	43
9	GEN	0.8345	41
10	IEN	0.7735	38
11	EST	0.7531	37
12	IDO	0.7124	35
13	ONT	0.6717	33
14	MEN	0.6310	31
15	ACI	0.6106	30
16	DOS	0.6106	30
17	INT	0.6106	30
18	ART	0.5903	29
19	ENI	0.5903	29
20	NID	0.5903	29
21	PER	0.5903	29
22	IAL	0.5496	27
23	ICA	0.5496	27
24	LDS	0.5496	27
25	RES	0.5496	27

Observamos que las letras que más se repiten en el texto 3 son la E, A, O e I , luego en menor medida la N, la S, R y la T. Las letras menos frecuentes son la Z, K, X y la W.

Explicación del análisis:

A partir de los datos anteriores, se puede decir que:

- Las consonantes más frecuentes son: N, S, R, T, C (aparecen con una frecuencia aprox un 30%)
- La E, la A y la O son identificables fácilmente dado su porcentaje de aparición.
- Las vocales ocuparán alrededor del 40% del texto.
- Las seis letras menos frecuentes son: H, J, Z, K, X, W (sumadas tienen una frecuencia que apenas supera el 1,73%)

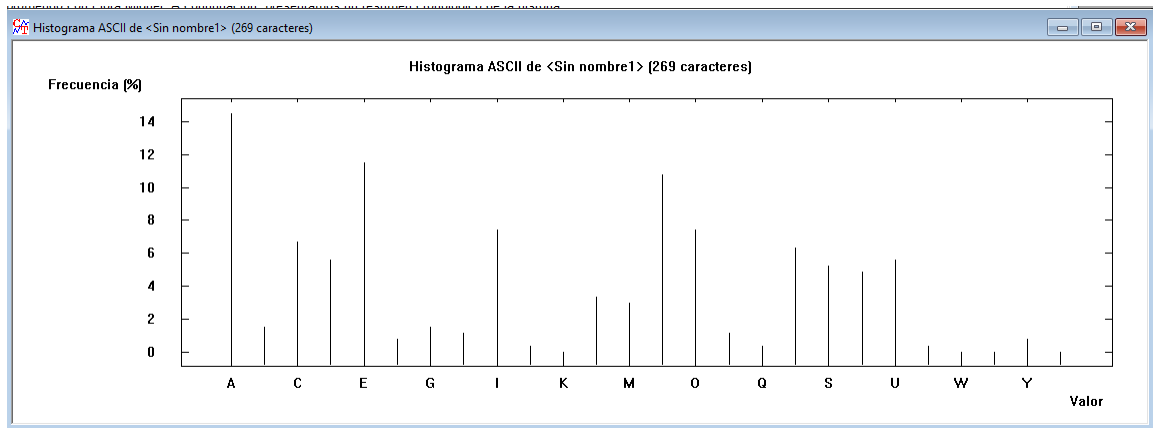
Al igual que en los diagramas anteriores, las vocales y las consonantes que más se repiten se parecen bastante debido a que todos los textos son en español.

Tarea 1-2

Tome una pequeña parte (aprox. 200 letras) de los mismos textos anteriores y recalcule las frecuencias.

Observa variaciones? Explique.

Para 268 Caracteres del texto 1



Lista de N-Gramas de Sin nombre1

Selección:

- ☐ Histograma (22)
- ☒ Dígrama (89)
- ☐ Trígrama (122)
- ☐ 4-grama (101)

Mostrar los 22

N-gramas más comunes (valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	DE	4.2654	9
2	EN	3.7915	8
3	UN	3.3175	7
4	CD	2.8436	6
5	IA	2.8436	6
6	CI	2.3697	5
7	ES	2.3697	5
8	NA	2.3697	5
9	RE	2.3697	5
10	IC	1.8957	4
11	LA	1.8957	4
12	NT	1.8957	4
13	ON	1.8957	4
14	TO	1.8957	4
15	AB	1.4218	3
16	AD	1.4218	3
17	AN	1.4218	3
18	AS	1.4218	3
19	AT	1.4218	3
20	CA	1.4218	3
21	CR	1.4218	3
22	DA	1.4218	3

Lista de N-Gramas de Sin nombre1

Selección

☐ Histograma (22)
☐ Digrama (89)
☒ Trígrama (122)
☐ 4 -grama (101)

Mostrar los 22

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

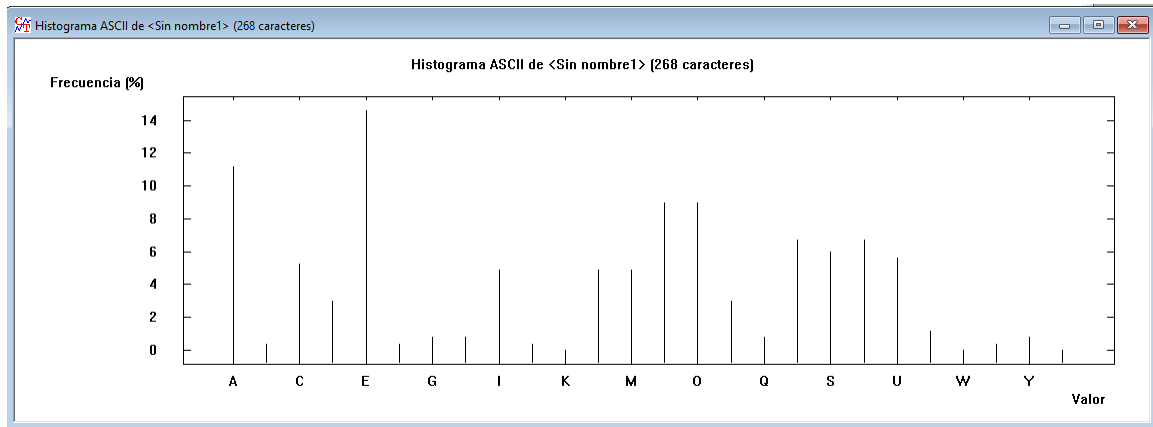
Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	CIA	1.8987	3
2	CON	1.8987	3
3	NCI	1.8987	3
4	RES	1.8987	3
5	ABA	1.2658	2
6	ACI	1.2658	2
7	ADA	1.2658	2
8	ANU	1.2658	2
9	END	1.2658	2
10	ERT	1.2658	2
11	ESU	1.2658	2
12	HIS	1.2658	2
13	IAD	1.2658	2
14	ICA	1.2658	2
15	ICO	1.2658	2
16	IEN	1.2658	2
17	IST	1.2658	2
18	MEN	1.2658	2
19	MUE	1.2658	2
20	NIC	1.2658	2
21	NTI	1.2658	2
22	NUN	1.2658	2

Explicación del análisis:

Podemos notar que hay mayores variaciones en el trígrama y Digrama. El histograma mantiene la frecuencia en las vocales ocuparán alrededor del 45% del texto.

Para 268 caracteres del Texto 2



Lista de N-Gramas de Sin nombre1

Selección

☐ Histograma (23)

☒ Digrama (107)

☐ Trigrama (137)

☐ 4 -grama (116)

Mostrar los 23

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	EN	4.2453	9
2	CO	2.8302	6
3	NT	2.8302	6
4	TA	2.8302	6
5	LA	2.3585	5
6	MU	2.3585	5
7	NO	2.3585	5
8	ON	2.3585	5
9	TE	2.3585	5
10	UE	2.3585	5
11	DE	1.8868	4
12	EL	1.8868	4
13	ER	1.8868	4
14	ES	1.8868	4
15	ME	1.8868	4
16	RE	1.8868	4
17	SE	1.8868	4
18	AS	1.4151	3
19	CI	1.4151	3
20	IA	1.4151	3
21	IM	1.4151	3
22	NC	1.4151	3
23	OC	1.4151	3

Lista de N-Gramas de Sin nombre1

Selección

☐ Histograma (23)

☐ Digrama (107)

☒ Trigrama (137)

☐ 4 -grama (116)

Mostrar los 23

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

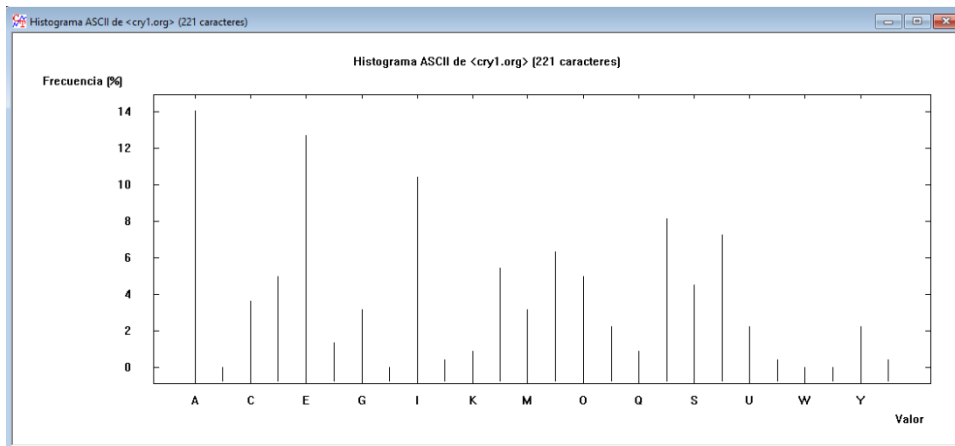
Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	ENT	3.1250	5
2	CON	1.8750	3
3	MUE	1.8750	3
4	CIA	1.2500	2
5	ENC	1.2500	2
6	ERT	1.2500	2
7	IME	1.2500	2
8	MEN	1.2500	2
9	NCI	1.2500	2
10	NTA	1.2500	2
11	NTE	1.2500	2
12	PRO	1.2500	2
13	QUE	1.2500	2
14	RIM	1.2500	2
15	RTE	1.2500	2
16	SEN	1.2500	2
17	TRA	1.2500	2
18	UER	1.2500	2
19	ACT	0.6250	1
20	ADR	0.6250	1
21	AGO	0.6250	1
22	AJE	0.6250	1
23	ALE	0.6250	1

Explicación del análisis:

No se encuentran tantas variaciones en la frecuencia porque el trigrama ENT y el digrama EN predominan en el párrafo.

Para 268 Caracteres del texto 3



Lista de N-Gramas de cry1.org

Selección

☒ Histograma (22)

☐ Digrama (75)

☐ Trigrama (96)

☐ 4 -grama (78)

Mostrar los 22

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	A	14.0271	31
2	E	12.6697	28
3	I	10.4072	23
4	R	8.1448	18
5	T	7.2398	16
6	N	6.3348	14
7	L	5.4299	12
8	D	4.9774	11
9	O	4.9774	11
10	S	4.5249	10
11	C	3.6199	8
12	G	3.1674	7
13	M	3.1674	7
14	P	2.2624	5
15	U	2.2624	5
16	Y	2.2624	5
17	F	1.3575	3
18	K	0.9050	2
19	Q	0.9050	2
20	J	0.4525	1
21	V	0.4525	1
22	Z	0.4525	1

Lista de N-Gramas de cry1.org

Selección

☐ Histograma (22)

☒ Digrama (75)

☐ Trigrama (96)

☐ 4 -grama (78)

Mostrar los

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	AR	3.9106	7
2	AL	2.7933	5
3	DE	2.7933	5
4	ES	2.7933	5
5	IG	2.7933	5
6	IN	2.7933	5
7	MA	2.7933	5
8	NT	2.7933	5
9	TI	2.7933	5
10	CI	2.2346	4
11	DA	2.2346	4
12	EL	2.2346	4
13	EN	2.2346	4
14	IA	2.2346	4
15	OS	2.2346	4
16	TA	2.2346	4
17	TE	2.2346	4
18	AN	1.6760	3
19	ER	1.6760	3
20	ET	1.6760	3
21	LA	1.6760	3
22	NO	1.6760	3

Lista de N-Gramas de cry1.org

Selección

☐ Histograma (22)

☐ Digrama (75)

☒ Trigrama (96)

☐ 4 -grama (78)

Mostrar los

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	CIA	2.8369	4
2	NTE	2.8369	4
3	INT	2.1277	3
4	TOS	2.1277	3
5	ARK	1.4184	2
6	ART	1.4184	2
7	ATO	1.4184	2
8	CES	1.4184	2
9	DAT	1.4184	2
10	DIG	1.4184	2
11	ELI	1.4184	2
12	ENC	1.4184	2
13	ESA	1.4184	2
14	ETI	1.4184	2
15	FIC	1.4184	2
16	GEN	1.4184	2
17	GIT	1.4184	2
18	IAL	1.4184	2
19	ICI	1.4184	2
20	IFI	1.4184	2
21	IGE	1.4184	2
22	IGI	1.4184	2

Explicación del análisis:

Se pueden encontrar variaciones en la frecuencia en los diagramas y en el trigrama, seguramente debido a que al tener una menor cantidad de caracteres las muestras tomadas no pueden reflejar los mismos patrones que los vistos al tomar una muestra de 10.000 caracteres debido a que la misma puede ser no representativa del todo el idioma español.

Tarea 1-3

Ídem **Tarea 1** pero en con textos en Ingles.

Se mantiene la distribución? Explique.

Histograma Texto 1 En Ingles

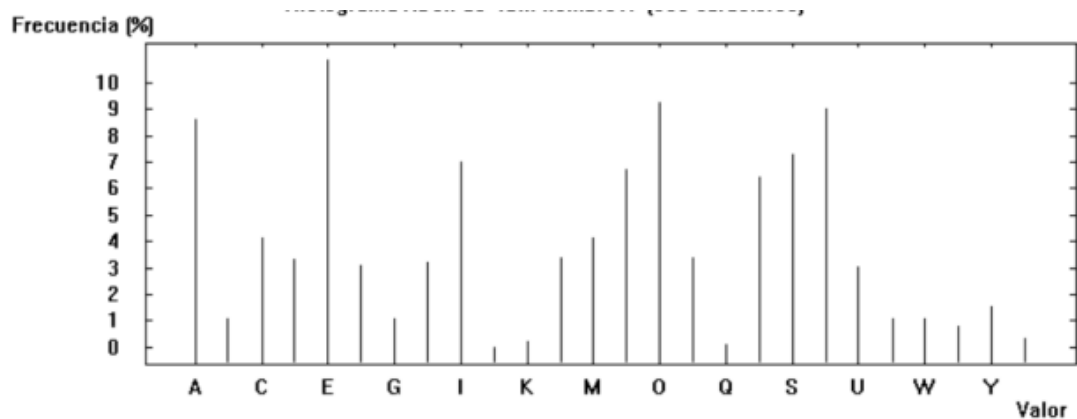


Diagrama texto 1 en Ingles

Lista de N-Gramas de Sin nombre1

Selección

☐ Histograma (25)

☒ Digrama (198)

☐ Trigramma (402)

☐ 4 -grama (376)

Mostrar los: 25

N-gramas más comunes:
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	IN	2.6895	22
2	AN	2.3227	19
3	OR	2.3227	19
4	TH	1.9560	16
5	ST	1.8337	15
6	HE	1.7115	14
7	OF	1.7115	14
8	ON	1.7115	14
9	RE	1.7115	14
10	TE	1.7115	14
11	TI	1.7115	14
12	ES	1.4670	12
13	FO	1.4670	12
14	MP	1.4670	12
15	AR	1.3447	11
16	AT	1.3447	11
17	CO	1.3447	11
18	ND	1.3447	11
19	OM	1.3447	11
20	AL	1.2225	10
21	RO	1.2225	10
22	HA	1.1002	9
23	LE	1.1002	9
24	PR	1.1002	9
25	SO	1.1002	9

Trigrama Texto 1 en Ingles

Lista de N-Gramas de Sin nombre1

Selección

☐ Histograma (25)
☐ Digrama (198)
☒ Trigrama (402)
☐ 4 -grama (376)

Mostrar los 25

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

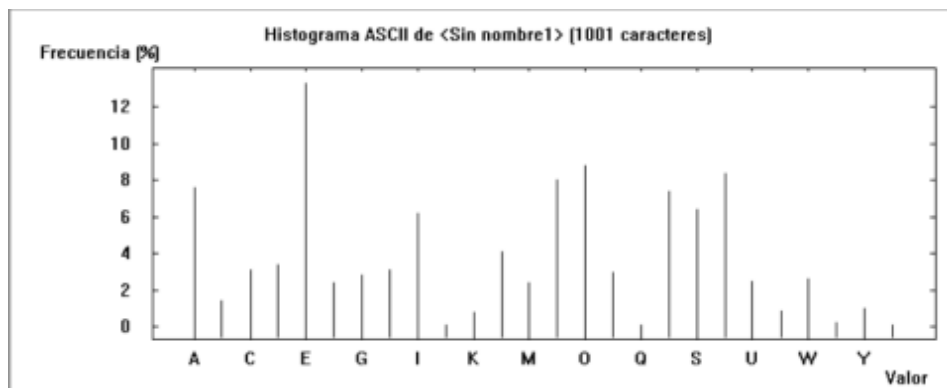
Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	THE	2.0155	13
2	FOR	1.5504	10
3	COM	1.3953	9
4	PRO	1.3953	9
5	ION	1.2403	8
6	OMP	1.2403	8
7	ORM	1.2403	8
8	TIO	1.2403	8
9	AND	0.9302	6
10	ATI	0.9302	6
11	ARE	0.7752	5
12	IST	0.7752	5
13	MPL	0.7752	5
14	PLE	0.7752	5
15	PUT	0.7752	5
16	RMA	0.7752	5
17	WAR	0.7752	5
18	FTW	0.6202	4
19	ICA	0.6202	4
20	INF	0.6202	4
21	LEX	0.6202	4
22	MAT	0.6202	4
23	NFO	0.6202	4
24	OFT	0.6202	4
25	ROV	0.6202	4

Histograma Texto 2 En Ingles



Histograma Texto 3 En Ingles

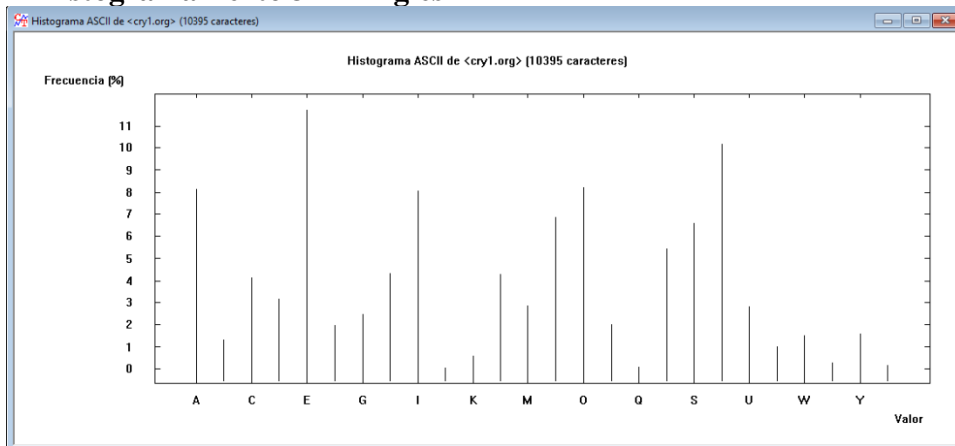


Diagrama texto 3 en Ingles

Lista de N-Gramas de cry1.org

Selección:

- ☐ Histograma (26)
- ☒ Digrama (309)
- ☐ Trigrama (1059)
- ☐ 4 -grama (1343)

Mostrar los 26

N-gramas más comunes (valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	TH	3.1272	261
2	HE	2.3844	199
3	IN	2.2765	190
4	ON	2.1927	183
5	AT	1.9530	163
6	ER	1.8931	158
7	TI	1.8692	156
8	TE	1.6894	141
9	AN	1.6535	138
10	ES	1.6535	138
11	EN	1.5696	131
12	RE	1.5217	127
13	NT	1.4977	125
14	CO	1.4019	117
15	ND	1.3180	110
16	OR	1.2221	102
17	AL	1.2102	101
18	TO	1.1383	95
19	OU	1.0784	90
20	IS	1.0664	89
21	ST	1.0544	88
22	IT	1.0424	87
23	NG	1.0304	86
24	OF	0.9945	83
25	HA	0.9705	81
26	AR	0.9585	80

Trigrama Texto 3 en Ingles

Lista de N-Gramas de cry1.org

Selección

☐ Histograma (26)
☐ Digrama (309)
☒ Trigrama (1059)
☐ 4 -grama (1343)

Mostrar los 26

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	THE	2.7672	175
2	AND	1.3757	87
3	ING	1.2334	78
4	ION	1.1860	75
5	CON	1.1227	71
6	ENT	0.9330	59
7	HAT	0.9171	58
8	NTE	0.8697	55
9	TIO	0.8223	52
10	YOU	0.7906	50
11	NCE	0.7116	45
12	ONS	0.6958	44
13	ATI	0.6325	40
14	VER	0.6167	39
15	ERS	0.6009	38
16	TEN	0.6009	38
17	THA	0.6009	38
18	RTI	0.5851	37
19	ATE	0.5534	35
20	RAT	0.5376	34
21	GEN	0.5218	33
22	ILL	0.5218	33
23	ENC	0.5060	32
24	ONT	0.5060	32
25	OUR	0.4744	30
26	FOR	0.4586	29

Explicación del análisis:

En los textos anteriores notamos similitudes entre ellos en cuanto a las letras que más se repiten: A, E, I, N, O, R, S, T;

Por otro lado, se visualiza que los diagramas se modifican y las frecuencias que más se repiten son OR, IN, EN, AN, TH

Para los trigramas se observa THE como dominante, y luego coincidencias como ARE.

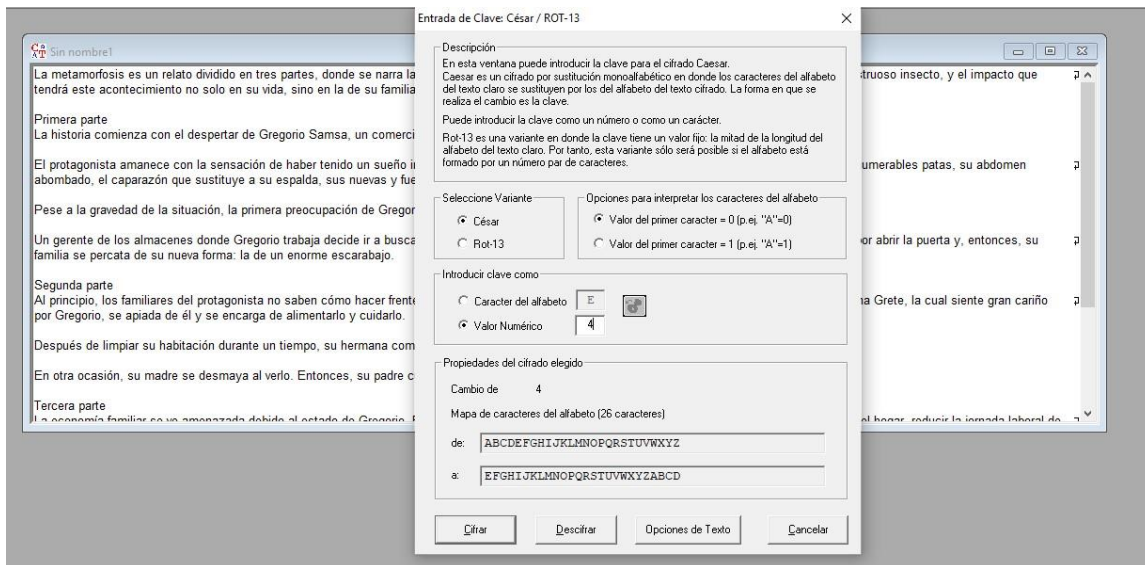
Tarea 1-4

Tome uno de los textos planos (ej Novela). Encripte tanto el texto corto como el texto largo de las tareas 1 y 2 mediante los cifrados clásicos que existen en Cryptool : *Caesar*, *Vigenere*, *Hill*, *Substitution*, *Playfair* y *Permutation*.

Encuentre las distribuciones de letras, diagramas y triagramas.

¿Se puede saber el cifrado empleado conociendo las frecuencias? Explique

Encriptación por Caesar clave 4



Pe qixeqsvjswmw iw yr vipexs hzmzhmhs ir xviw tevxiw, hsrhi wi revve pe xverwjsvqegmór hi Kviksvms Weqwe, yr zmenerxi hi gsqivgms hi xipew, ir yr qsrwxvysws mrwigxs, c ip mqtexgs uyi xirhvá iwxi egxrigmqmirxs rs wps ir wy zmhe, wmrs ir pe hi wy jeqmpme.

Tvmqive tevxi

Pe lmwxsvme gsqmirde gsr ip hiwtivxev hi Kviksvms Weqwe, yr gsqivgmep irgevkehs hi qerxiriv igsróqmgeqirxi e xshe wy jeqmpme.

Ip tvsxeksrnwxe eqerigi gsr pe wirwegmór hi lefiv xirmhs yr wyiñs mrxveruymys. Tsqs e tsqs, ze hiwgyfvmirhs wy xverwjsvqegmór ir yr mrwigxs: wyw mrryqivefpiw texew, wy efhsqir efsqfehs, ip getevedór uyi wywxmxyxi e wy iwtephe, wyw ryizew c jyivxiw qerhífypew.

Tiwi e pe kvezihew hi pe wmxyegmór, pe tvmqive tvisgytegmór hi Kviksvms iw nywxmjmgev wy iwxehs ir ip xvefens.

Yr kivirxi hi psw epqegiriw hsrhi Kviksvms xvefene higmhi mv e fywgevps e wy gewe hifmhs e wy mrywyep vixvews. Ip tvsxeksrnwxe legi yr kver iwjyivds tsv efvmv pe tyivxe c, irxsrgiw, wy jeqmpme wi tivgexe hi wy ryize jsvqe: pe hi yr irsvqi iwgevefens.

Wikyrhe tevxi

Ep tvmrgmtms, psw jeqmpmeviw hip tvsxeksrnwxe rs wefir góqs legiv jvirxi e pe ryize wxxyegmór. Wy tehvi wi irjehe c ps hiwtvigme. Wmr iqfevks, wy livqere Kvixi, pe gyep wmirxi kver gevniñs tsv Kviksvms, wi etmehe hi ép c wi irgevke hi epmqirxevps c gymhevps.

Hiwtyéw hi pmqtmev wy lefmxegmór hyverxi yr xmiqts, wy livqere gsqmirde e vityhmevps.

Ir sxve sgewmór, wy qehvi wi hiwqece ep zivps. Irxsrgiw, wy tehvi gypte ep iwgevefens hi ps wygihmhs c pi perde qerderew teve egvmfmppevpi.

Xivgive tevxi

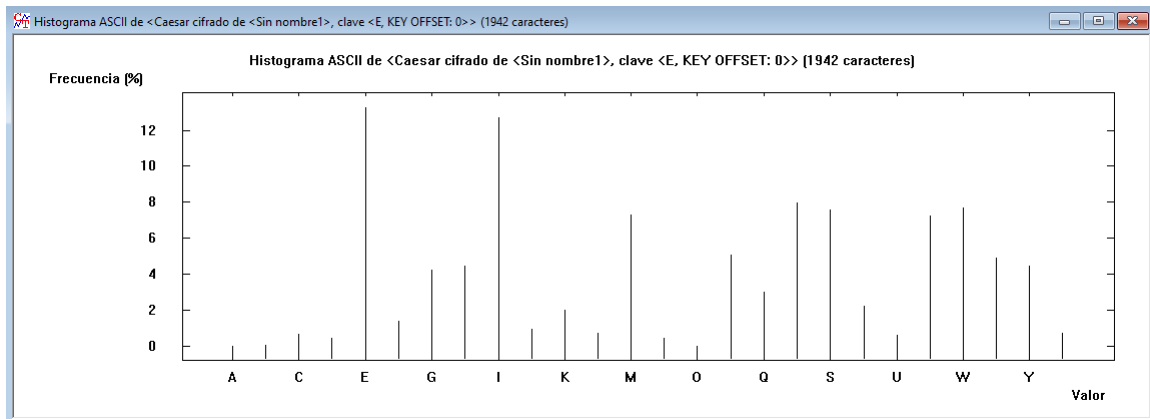
Pe igrsqíe jeqmpmev wi zi eqiredehe hifmhs ep iwxehs hi Kviksvms. Irxsrgiw, wyw qmiqfvsw xmirir uyi viepmdew epkyrsw enywxiiw: vigsvxev psw kewxsw hip lskev, vihygm v pe nsvrehe pefsvpe hi pe gvmehe c epuympev yre hi pew lefmxegmsriw e ryizsw mruympmrsw.

Pe wxxyegmór gsr psw mruympmrsw kirive gsrjpmgxsw ir ip lskev. Tyiw, iwxs wsr qyc ibmkirxiw gsr pe pmqtmide c pe jeqmpme mxirxevá qerxiriv e Kviksvms ir wigvixs.

Yre rsgli, Kvixi xsge ip zmspír teve psw mrzmxehsw c Kviksvms, e uymir pi irgerxe wy qúwmge, higmhi mv ep wepór. Tvsrxs, ip mrwigxs iw hiwgyfmivxs tsv psw mruympmrsw, uymiriw xivqmrrer eferhsrerhs pe gewe wmr tekev wy iwxxergme.

Hiwtyéw hi iwxi ligls, pe jeqmpme irxmrihi uyi pe wxxyegmór hi Kviksvms iw mrwsxirmfpi. Ip tvsxeksrnwxe xeqfmér ps gvii ewí, hi qshs uyi higmhi irgivvevwi hijmrmxmzeqirxi ir wy

lefmxegmór wmr epmqirxewi. Híew qáw xevhi, pe gymehe ps irgyirxve qyivxs.



Selección

- ☒ Histograma (24)
☐ Digrama (193)
☐ Trigramas (530)
☐ 4 -grama (575)

Mostrar los 24

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	E	13.2853	258
2	I	12.7188	247
3	R	7.9815	155
4	W	7.6725	149
5	S	7.5695	147
6	M	7.3120	142
7	V	7.2091	140
8	P	5.0463	98
9	X	4.8919	95
10	Y	4.4799	87
11	H	4.4284	86
12	G	4.2225	82
13	Q	2.9866	58
14	T	2.2142	43
15	K	2.0082	39
16	F	1.3903	27
17	J	0.9269	18
18	L	0.7209	14
19	Z	0.7209	14
20	C	0.6694	13
21	U	0.6179	12
22	D	0.4634	9
23	N	0.4119	8
24	B	0.0515	1

Lista de N-Gramas de Caesar cifrado de <Sin nombre1>, clave <E, KEY OFFSET: 0>



Selección

☐ Histograma (24)

☒ Digrama (193)

☐ Trigramas (530)

☐ 4 -grama (575)

Mostrar los

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	IR	3.3641	51
2	HI	2.9024	44
3	IW	2.3747	36
4	EV	2.2427	34
5	PE	1.9789	30
6	VI	1.8470	28
7	XI	1.8470	28
8	WY	1.7810	27
9	XE	1.7810	27
10	IV	1.6491	25
11	VE	1.6491	25
12	RX	1.5831	24
13	MR	1.4512	22
14	SR	1.4512	22
15	ER	1.3852	21
16	GM	1.3852	21
17	SV	1.3852	21
18	SW	1.2533	19
19	VM	1.2533	19
20	XS	1.2533	19
21	EG	1.1214	17
22	EP	1.1214	17
23	HS	1.1214	17
24	ME	1.1214	17

Lista de N-Gramas de Caesar cifrado de <Sin nombre1>, clave <E, KEY OFFSET: 0>



Selección

☐ Histograma (24)

☐ Digrama (193)

☒ Trigrama (530)

☐ 4 -grama (575)

Mostrar los

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	IRX	1.3181	15
2	RXI	1.0545	12
3	EGM	0.9666	11
4	KVI	0.9666	11
5	MPM	0.8787	10
6	SVM	0.8787	10
7	IKS	0.7909	9
8	KSV	0.7909	9
9	MIR	0.7909	9
10	VIK	0.7909	9
11	VMS	0.7909	9
12	GSR	0.7030	8
13	XVE	0.7030	8
14	EQM	0.6151	7
15	GEV	0.6151	7
16	HIW	0.6151	7
17	JEQ	0.6151	7
18	PME	0.6151	7
19	QER	0.6151	7
20	QMP	0.6151	7
21	TEV	0.6151	7
22	UYM	0.6151	7
23	WXE	0.6151	7
24	EHE	0.5272	6

Encriptación por Vignere

Entrada de Clave: Vigenère



Introduzca la clave.
¡La longitud máxima de clave es de 1024 caracteres!

Cifrar Descifrar Opciones de Texto Salir

Ar qqbobfvrgxj ie cb gvpmbc szzulwsf iz bftj tmzhtj, havrt ji zifgr pm bfpewrwfbrguón rt
Xvqocgzs Eiahr, yz dwpaezbs sv gausgtma ls ivpma, sc lr ywbhkvvgwd zremqif, c qt wbgeobc fli
fmbsiá iebz ptszbsrzqumbif ra acaf iz ai kzhm, awcf iz to sv wg nobzpui.

Dgzqqzo ervfm

Zp ymebcgze owaxvrli qde ix lshgidbog ui Szsvfvuw Gpdwm, cb rfqqzqxrpx qvpikmlc sv qmvhteid
mqdeóqukobvrfm o ifhm ai urqutwp.

Vp bzcirkavwhke muocvgq kcc ce embhrguón rt yenmf ivrulc je wgmñc xexdibflmxw. Ddts m xcrf, zm lshtynzwteha ai iiezatdiqmkwóc vr gv wcjiobc: hlw uvbjdidipavw bihpj, wg ipsfqqv oqfqnrld, vp oidpielón ejv wgahxkykm o hl iexoaue, ecg clihig n wyqzhtj qmvríqlpma.

Dtji m to viehmrpu hq to hzxgiqxóe, pm xfxdidi dgvsocdptmóz ls Viiswxf ie rihkmrqqpi wg mgirha mb tc xdippas.

Gv utiizbs sv paa oadeombtj havrt Xvqocgzs fzoqnm lsrzhq qf p syekogcs m ai rrwm lsqzha i gj zrgaipc vqbfpps. Qt dgfxmocczwfi vpti gv ugrr qatjvvlw ddi enzwg ce bcsge k, mbifromg, hl jmuwaze em dtigmbó sv wg vitme rwfbr: pm ls je izwfbv iekogrfmrc.

Hvkgvrp gedbs

Pc tdqbrztuw, zdj jmuwazedmg svp bzcirkavwhke zw gpsiz kóad yeomf uiizbs p ce zcskr wubiptmóz. Ai erhdm gt vrrirp p pa lshgvqkw. Jmz maqrsvw, gj yiduocr Kdmht, ce ocoa jmqvht xvmv qpimña xcg Xvqocgzs, em oezepi rt éc c em sctedoo sv exqatexmzzd p ggqrpipa.

Lshgyée ls azqbqog jy tipxkeoqób slvmvht lr fqsbg, ec vtiqmvo rfqumbor e dmdjummzzd.

Vr abfp fgmawóc, jy yirgv wq lshdeki oa midtc. Texavqtj, wg xosii oczer ex mgrrvmjjoyf hq tc hlgqlwsf c xm zpedm uocqezig ervm iqgzfutzpipq.

Bsgtidi dpixq

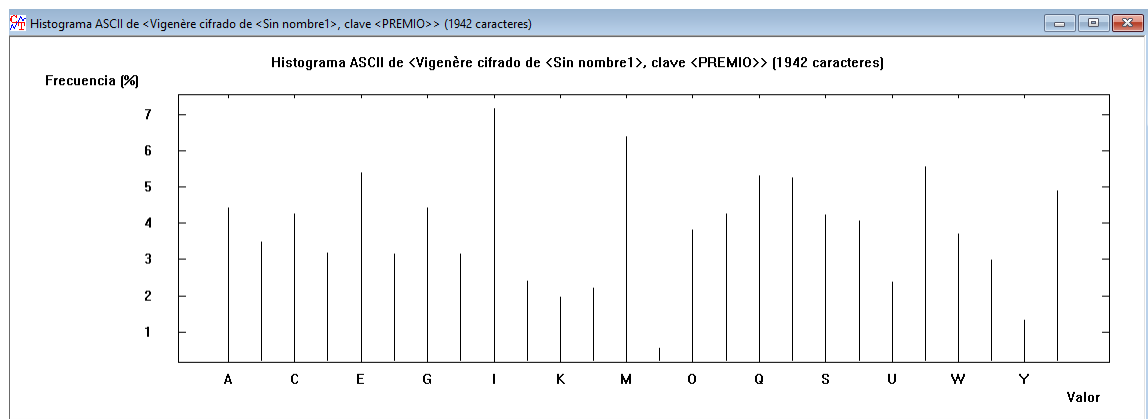
To ttszwaíp weyqzrv em jt rqqvoorhm lsqzha iz tjxmlc sv Kdmudima. Mbifromg, hlw yqbsbvaa hxvrqv ejv vqizxqed izvlraa oylwfm: gvgazhpi paa upjxaa rtc laoog, iipcxi pm rcgeepi zpssdz sv pm kfxrhg oahyutog lrm ls arw tipxkeoqccvw m vitmse qbflmxqbdj.

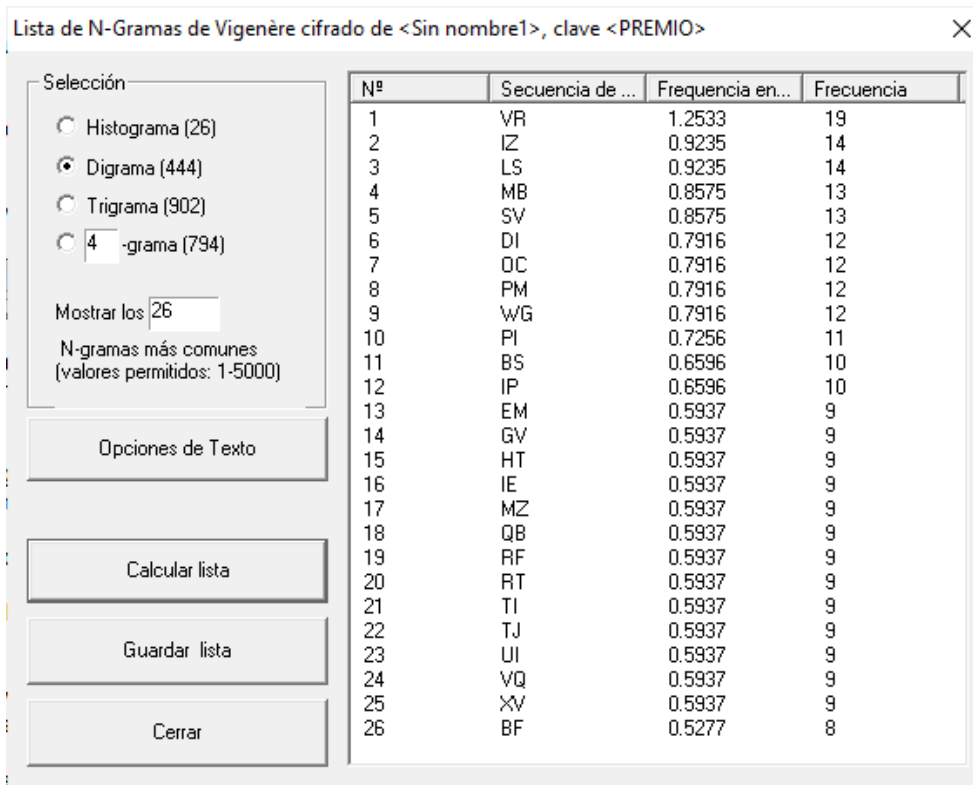
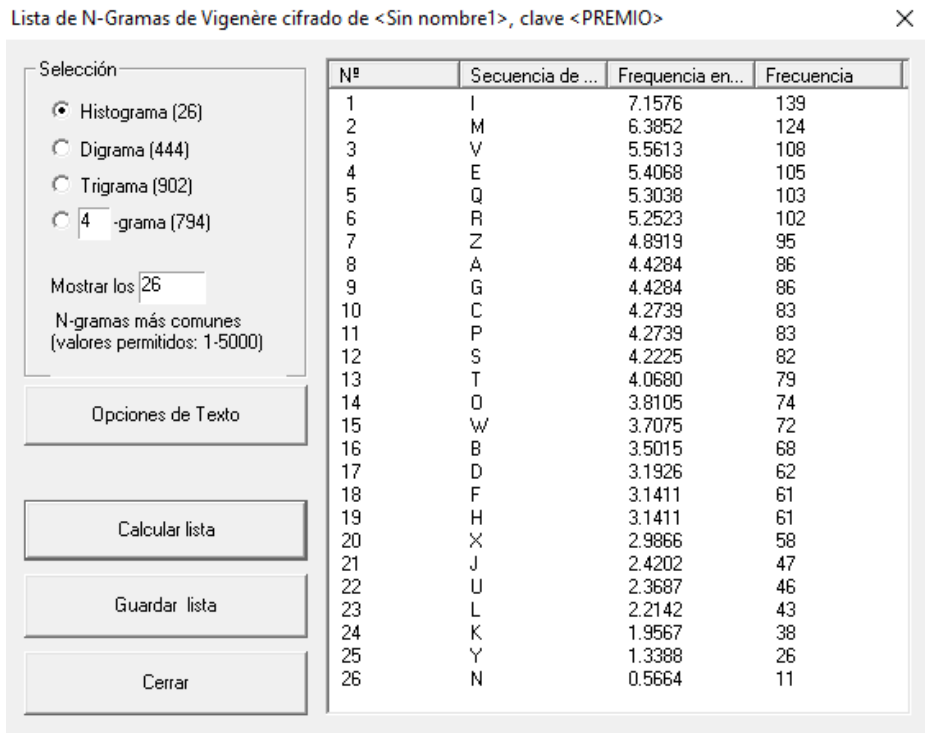
Pm awileoqób rfr xwg xeugqzese oscvmm kccwpukhdj iz mz wfkmm. Djvw, qahdj wav ajp ijqutexqa qde pm twbgmqho n ce riexcmm qbivrfifá brfmbti e Szsvfvuw sc jiozsif.

Yzi bdtlq, Oftki fwqp vp hqcaíe tmzo afw uvjxkepww n Xvqocgzs, m yixvr xm sctezbo hl quéeqp, uioqrt zv mt gpcór. Bzccks, qt wcjiobc tj hqaqjmqzhd gsd tch zrcwazraa, ejzizmg ivvyqbpe enibsfmrvrd ce oigp jmz xovrv ec shkezkw.

Uiexiéh ui qaht yiopc, ar jmuwaze qvhxvrpm ejv pm awileoqób sv Kdmudima mg xewaahtemnts.

Tc tdwhpxszqgir xmupxée pa kftv eel, ls bfha yit uioqrt vromfgrvem rtwmzqhxmeymbiv iz ai wrfuborzór eqb pcmymbirvem. Rípj qáe bogui, xi qgzepi zd vrocckvm uitixa.





Lista de N-Gramas de Vigenère cifrado de <Sin nombre1>, clave <PREMIO>



Selección

☐ Histograma (26)

☐ Digrama (444)

☒ Trigramma (902)

☐ 4 -grama (794)

Mostrar los 26

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	CGZ	0.4394	5
2	LSH	0.4394	5
3	MBI	0.4394	5
4	EOQ	0.3515	4
5	GZS	0.3515	4
6	OCG	0.3515	4
7	QDC	0.3515	4
8	QZH	0.3515	4
9	VQO	0.3515	4
10	WAZ	0.3515	4
11	XVQ	0.3515	4
12	XVR	0.3515	4
13	ZBS	0.3515	4
14	AVW	0.2636	3
15	AZE	0.2636	3
16	BFP	0.2636	3
17	BIF	0.2636	3
18	BZC	0.2636	3
19	EJV	0.2636	3
20	EPI	0.2636	3
21	HKE	0.2636	3
22	IDI	0.2636	3
23	JIO	0.2636	3
24	JMU	0.2636	3
25	KDM	0.2636	3
26	MUW	0.2636	3

Encriptación por Hill

Entrada de Clave: Algoritmo de Hill

Descripción

El cifrado de Hill es un cifrado por sustitución polialfabético basado en álgebra lineal.

Fue el primer sistema criptográfico polialfabético que era práctico para trabajar con más de tres símbolos simultáneamente.

Se divide el texto en bloques de d elementos que son tratados como vectores d -dimensionales. La clave es una matriz aleatoria $d \times d$ inversible en \mathbb{Z}_{26} .

Alfabeto usado (26 caracteres)

ABCDEFGHIJKLMNOPQRSTUVWXYZ

El primer caracter del alfabeto

0

Matriz Clave

☒ Caracteres del Alfabeto

☐ Valores Numéricos

Caracteres del Alfabeto

L

G

F

R

Valores Numéricos

11

06

05

17

Generar Clave Aleatoria

Reiniciar

Variantes

☐ (vector fila) * (matriz)

☒ (matriz) * (vector columna)

Tamaño de la Matriz

☐ 1 x 1

☒ 2 x 2

☐ 3 x 3

☐ 4 x 4

☐ 5 x 5

Matriz más Grande

☐ Mostrar detalles y pasos del proceso de cifrado H

Cifrar

Descifrar

Opciones Hill

Opciones de Texto

Cancelar

Hy qtrmyhzjshed mj ce tshyxq tqjctqdo ic ppmj zsfnmj, dovhm ji coyvc hy ppqikomqsdilóv hs Ntskdri Hkrgh, ce jcSSIPc va sjqthkgn va pchye, xt kx eoaqsleshk thcuxxq, s bd eeycdxq azs aicvná mjpc cdoapcilojicxq jm mInc ic wj jcxk, cnjm ic hy va wj tuojdec.

Qriqtvc zsfnw

Ug kedxqric dijyzxrc doa wu vascgsrmn bs Ntskdri Hkrgh, ce sjqthkajf opqoyezdo va sdnctigs uxoaóojmfqtnti p xqXk wj tuojdeo.

Lt tbgrmkdzoqsq vsdbykv sjr nu picghilóv hy ewmgs pczodo ce wjoñt awppqiazooa. lavo n fwsj, nw waspiiriicdo wj ppqikomqsdilób yt kz ohcuxxq: wjc ndvwnqswmfos cagup, wj wmdoqtd iheyuium, dt gcqoykeóv uah wjqskuqji p wj mJzszxu, pgl tkeiup y sahfnmj sdvhírchys.

Cmji p hy ccmoaoui va hy cnhocdaów, hy xvufgsc qtsavomcdaów va Ccsnmqgn mj bqqseqmroy wj mjrmdo ic wu ppwmsse.

Pn ggsicpc va ncg hbucdicmj dovhs Ntskdriy yvcbalo vailva ym w mglmfjho n wj mfgH vaxgdo u py xtkwjea tsspupm. Dt tbgrmkdzoqsg kcdy rn gvcb ykoahpla imq wmrj hc qahfne n, icxqpqmj, wj tuojdeu pu kgsfrm va wj tkeiu cmqsd: hy va ce icmqqt mjmfvcbars.

Exubvhc qoypc

Ea xvawilvyc, ssh tuojdeoymj vat tbgrmkdzoqsq is hwmic góbe ccdgs rxicpc e aq iahnw cnhocdaów. Wj zsvnm jg fhpiue n nc vasctsilu. Paw clbafas, hs ggssddi Ccsaw, uc dcrl syznTs nvcp qoygñn fwf Atskdri, hi pvyiui uw éu y fg fpqoyez va eauficrmjhc f chsioync.

Vascgél va deeyajz ws gwmkucdaów nmvcnty rn tyzeys, hs ggssddi sjojicfq o yukuqajjhm.

Dj mppw zmfcnóh, cw niuts ex vaadenq vd rgsnc. lcxqpqmj, wj zsvnu xqwzs ea mjmfvcbars va nc wjkvtqdo i qw uqifq sdxrqiup zsvc cdrixgvdo yfo.

Pchkgsc qoypc

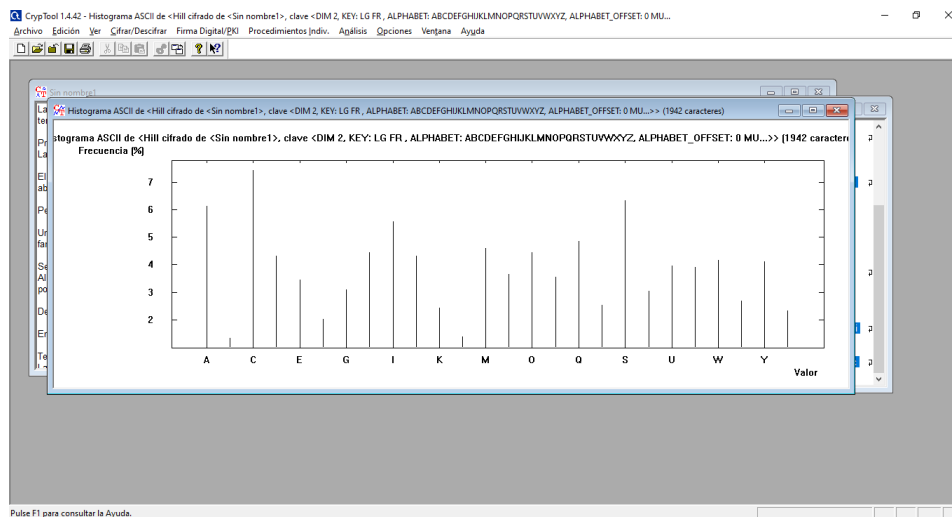
Hy uxoiijú ckrooajz we ii pqt difq xk vaxgdo ea mjrmdo va Ccsnmqgn. lcxqpqmj, wja dzyubgq syzbyv uah tseausoy eaubjmg hbqqsmj: tssjfnoy ncq fupxqy gwu viezt, faoozym hy rsvpiue awmmqea va hy kiajxk u lzkyxhyl edi va hyw wwwkucdgnbyg h tkeish awazooawsh.

Hy cnhocdaów sjr nsh awazooawsh cpbyvc sjhpdewqsh ic wu viezh. Xahe, xqssh mlx eqj qqkhicpcs poa hy deeyyzfq i qu ckrooaj awpcntoyá sdnticgs a Ttskdrim dh cuxtsxq.

Ceq iavnu, Ccsas aavo ld rgnhíl zsvc ncc nzbkuiush e Jtskdrio, n azyzr ng fpqqirm wj wúxmri, uuxsie vv cl seaóp. Dbgntm, dd ehcuxxq mj vasp iyzfna imq ncc nvuyxdejmy, tyxicmj pcpyawqi wmqidodivhc sc dupu paw zsezz wa hqsqiili.

Umjpuéy gg fqsy euxvi, hy tuo jdeo Intyzvha bah hy cnhocdaów va Ccsnmqgn mj awmlqsicgafo.

Wu xvyvatoaedrm rmyuaéw nc kigf upí, va yhdo aza ouxsig fpqgsvczwa omwawkuwckricpc ic wj pexgrmilóh caw eauficrmzwa. Óíup wáx rmnbw, uc driiue am dpqahntvc ifgsxq.



Lista de N-Gramas de Hill cifrado de <Sin nombre1>, clave <DIM 2, KEY: LG FR, ALPHABET: ABCD... X

Selección

☒ Histograma (26)

☐ Digrama (444)

☐ Trigrama (802)

☐ 4 -grama (703)

Mostrar los 26

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	C	7.4150	144
2	S	6.3337	123
3	A	6.1277	119
4	I	5.5613	108
5	Q	4.8404	94
6	M	4.5829	89
7	H	4.4284	86
8	O	4.4284	86
9	D	4.3254	84
10	J	4.3254	84
11	W	4.1710	81
12	Y	4.1195	80
13	U	3.9650	77
14	V	3.9135	76
15	N	3.6560	71
16	P	3.5530	69
17	E	3.4501	67
18	G	3.0896	60
19	T	3.0381	59
20	X	2.6777	52
21	R	2.5232	49
22	K	2.4202	47
23	Z	2.3172	45
24	F	2.0082	39
25	L	1.3903	27
26	B	1.3388	26

Lista de N-Gramas de Hill cifrado de <Sin nombre1>, clave <DIM 2, KEY: LG FR, ALPHABET: ABCD... X

Selección

- ☐ Histograma (26)
☒ Digrama (444)
☐ Trigramas (802)
☐ 4 -grama (703)

Mostrar los 26

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	VA	1.9129	29
2	IC	1.8470	28
3	MJ	1.5172	23
4	HY	1.3193	20
5	WJ	1.3193	20
6	DO	1.1214	17
7	XQ	1.0554	16
8	AW	0.9894	15
9	GS	0.9894	15
10	QS	0.9894	15
11	RM	0.9894	15
12	TS	0.9894	15
13	CD	0.9235	14
14	QA	0.9235	14
15	OY	0.9235	14
16	PC	0.9235	14
17	RI	0.9235	14
18	VC	0.8575	13
19	NT	0.7916	12
20	PQ	0.7916	12
21	IU	0.7256	11
22	MQ	0.7256	11
23	SH	0.7256	11
24	WM	0.7256	11
25	DE	0.6596	10
26	EA	0.6596	10

Lista de N-Gramas de Hill cifrado de <Sin nombre1>, clave <DIM 2, KEY: LG FR, ALPHABET: ABCD... X

Selección			
<input type="radio"/>	Histograma (26)		
<input type="radio"/>	Digrama (444)		
<input checked="" type="radio"/>	Trigrama (802)		
<input type="radio"/>	4 -grama (703)		
Mostrar los 26			
N-gramas más comunes (valores permitidos: 1-5000)			
Opciones de Texto			
Calcular lista			
Guardar lista			
Cerrar			

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	DRI	0.7030	8
2	CDA	0.5272	6
3	KDR	0.5272	6
4	QOY	0.5272	6
5	SKD	0.5272	6
6	TSK	0.5272	6
7	CCS	0.4394	5
8	JDE	0.4394	5
9	OJD	0.4394	5
10	ODA	0.4394	5
11	TUO	0.4394	5
12	UOJ	0.4394	5
13	VAS	0.4394	5
14	CNH	0.3515	4
15	CPC	0.3515	4
16	CUX	0.3515	4
17	CXQ	0.3515	4
18	EAU	0.3515	4
19	GRM	0.3515	4
20	HOC	0.3515	4
21	ICG	0.3515	4
22	ICP	0.3515	4
23	ICX	0.3515	4
24	NHO	0.3515	4
25	NTS	0.3515	4
26	OCD	0.3515	4


Encriptación por Sustitución

Entrada de Clave: Sustitución Monoalfabética/ Atbash

Elija una variante de la sustitución monoalfabética

☒ A partir de la clave y manteniendo el resto de caracteres en orden ascendente
☐ A partir de la clave y manteniendo el resto de caracteres en orden descendente
☐ Atbash (se utiliza una clave fija)

Clave a utilizar

Clave: 

Offset:

Información sobre la Sustitución a Realizar

El alfabeto (26 caracteres) será

desde:

hasta:

Ip jatpjlqblfr ar uk qaiptl ofvfofol ak tqar mpqtar, olkoa ra kpqqp ip tqpkrlqjpsfók oa Cqaclql Rpjrp, uk vfpqpkta oa sljaqsfl oa taipr, ak uk jlqrtulrl fkrastl, y ai fjmpstl nua takoqá arta psltkasfjaktl kl rlil ak ru vfop, rfkl ak ip oa ru bpjfifp.

Mqfjaqp mpqta

Ip dfrtlqfp sljfakzp slk ai oarmaqtpq oa Cqaclql Rpjrp, uk sljaqsfpi akspqcpol oa jpktakaq askójsfjakta p tlop ru bpjfifp.

Ai mqltpclkrtp pjpkasa slk ip rakrpsfók oa dpeaq takfol uk ruañl fktqpknufil. Mlsl p mlsl, vp oarsueqfakol ru tqpkrlqjpsfók ak uk fkrastl: rur fkkujaqpeiar mptpr, ru peoljak peljepol, ai spmpqpszók nua rurtftuya p ru armpiop, rur kuavpr y buaqtar jpkoíeuipr.

Mara p ip cqpvapo oa ip rftupsfók, ip mqfjaqp mqalsumpsfók oa Cqaclql ar gurtfbfspq ru artpol ak ai tqpepgl.

Uk caqakta oa ilr pijpsakar olkoa Cqaclql tqpepgp oasfoa fq p eurspqil p ru sprp oaefol p ru fkurupi qatqprl. Ai mqltpclkrtp dpsa uk cqpk arbuaqzl mlq peqfq ip muaqtp y, aktlsar, ru bpjfifp ra maqsptp oa ru kuavp blqjp: ip oa uk aklja arspqpepgl.

Racukop mpqta

Pi mqfksfmfl, ilr bpjfifpqr oai mqltpclkrtp kl rpeak sójl dpsaq bqakta p ip kuavp rftupsfók. Ru mpoqa ra akbpop y il oarmqasfp. Rfk ajepqcl, ru daqjpkp Cqata, ip supi rfakta cqpk spqfñl mlq Cqaclql, ra pmfpop oa éi y ra akspqcp oa pifjaktpqil y sufopqil.

Oarmuér oa ifjmfqp ru dpeftpsfók ouqpkta uk tfajml, ru daqjpkp sljfakzp p qamuofpqil.

Ak ltqp lsprfók, ru jpoqa ra oarjpyp pi vaqil. Aktlsar, ru mpoqa suimp pi arspqpepgl oa il rusaofol y ia ipkzp jpkzpkpr mpqp psqfepiqia.

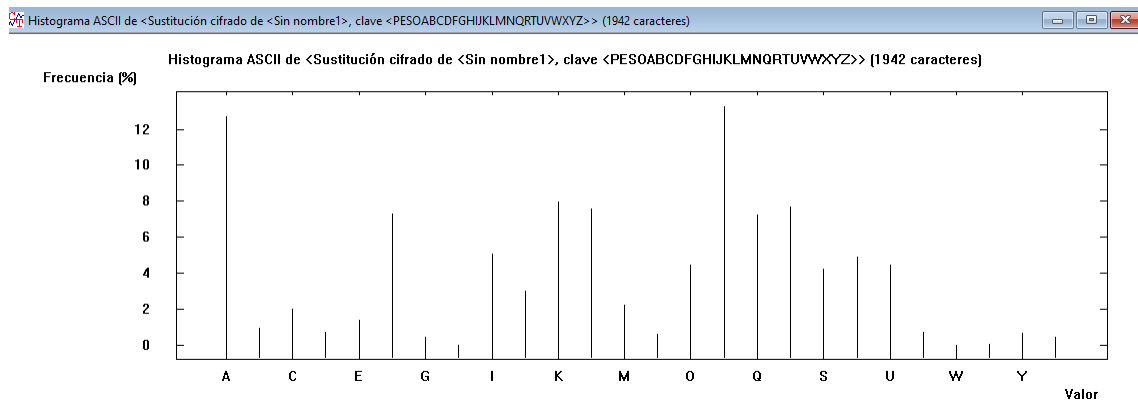
Taqaqp mpqta

Ip askljíp bpjifipq ra va pjakpzpop oaefol pi artpol oa Cqaclqfl. Aktlksar, rur jfajeqlr tfakak nua qapifzpq picuklr pgurtar: qasltqpq ilr cprtlr oai dlcpq, qaousfq ip glqkpop ipelqpi oa ip sqfpop y pinufipq ukp oa ipr dpeftpsflkar p kuavlr fknufifklr.

Ip rftupsfók slk ilr fknufifklr cakaqp slkbifstlr ak ai dlcpq. Muar, artlr rlk juy axfcaktar slk ip ifjmfazp y ip bpjifip fktaktppá jpktakaq p Cqaclqfl ak rasqatl.

Ukp kllda, Cqata tllsp ai vfliík mpqp ilr fkvftpolr y Cqaclqfl, p nufak ia akspktp ru júrfsp, oasfoa fq pi rpiók. Mqlktl, ai fkrastl ar oarsuefaqtl mlq ilr fknufifklr, nufakar taqjfkpk pepkolkpkol ip sprp rfk mpcpq ru artpksfp.

Oarmuér oa arta dasdl, ip bpjifip aktfakoa nua ip rftupsfók oa Cqaclqfl ar fklrltakfeia. Ai mqltpclkrtp tpjefék il sqaa prí, oa jlol nua oasfoa aksaqqpqa oabfkftvpjakta ak ru dpeftpsfók rfk pifjaktpqra. Oípr jár tpqoa, ip sqfpop il aksuaktqp juaqtl.



Lista de N-Gramas de Sustitución cifrado de <Sin nombre1>, clave <PESOABCDGHIJKLMNOPRTU... X

Selección

- ☒ Histograma (24)
☐ Digrama (193)
☐ Trigrama (530)
☐ 4 -grama (575)

Mostrar los 24

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Itexto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	P	13.2853	258
2	A	12.7188	247
3	K	7.9815	155
4	R	7.6725	149
5	L	7.5695	147
6	F	7.3120	142
7	Q	7.2091	140
8	I	5.0463	98
9	T	4.8919	95
10	U	4.4799	87
11	O	4.4284	86
12	S	4.2225	82
13	J	2.9866	58
14	M	2.2142	43
15	C	2.0082	39
16	E	1.3903	27
17	B	0.9269	18
18	D	0.7209	14
19	V	0.7209	14
20	Y	0.6694	13
21	N	0.6179	12
22	Z	0.4634	9
23	G	0.4119	8
24	X	0.0515	1

Lista de N-Gramas de Sustitución cifrado de <Sin nombre1>, clave <PESOABCDGHIJKLMNOPQRTU... X

Selección

- ☐ Histograma (24)
- ☒ Digrama (193)
- ☐ Trigrama (530)
- ☐ 4 -grama (575)

Mostrar los 24

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	AK	3.3641	51
2	QA	2.9024	44
3	AR	2.3747	36
4	PQ	2.2427	34
5	IP	1.9789	30
6	QA	1.8470	28
7	TA	1.8470	28
8	RU	1.7810	27
9	TP	1.7810	27
10	AQ	1.6491	25
11	QP	1.6491	25
12	KT	1.5831	24
13	FK	1.4512	22
14	LK	1.4512	22
15	LQ	1.3852	21
16	PK	1.3852	21
17	SF	1.3852	21
18	LR	1.2533	19
19	QF	1.2533	19
20	TL	1.2533	19
21	FP	1.1214	17
22	IL	1.1214	17
23	OL	1.1214	17
24	PI	1.1214	17

Lista de N-Gramas de Sustitución cifrado de <Sin nombre1>, clave <PESOABCDGHIJKLMNOPQRTU... X

Selección

☐ Histograma (24)
☐ Digrama (193)
☒ Trigrama (530)
☐ 4 -grama (575)

Mostrar los 24

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	AKT	1.3181	15
2	KTA	1.0545	12
3	CQA	0.9666	11
4	PSF	0.9666	11
5	FIF	0.8787	10
6	LQF	0.8787	10
7	ACL	0.7909	9
8	CLQ	0.7909	9
9	FAK	0.7909	9
10	QAC	0.7909	9
11	QFL	0.7909	9
12	SLK	0.7030	8
13	TQP	0.7030	8
14	BPJ	0.6151	7
15	IFP	0.6151	7
16	JFI	0.6151	7
17	JPK	0.6151	7
18	MPQ	0.6151	7
19	NUF	0.6151	7
20	OAR	0.6151	7
21	PJF	0.6151	7
22	RTP	0.6151	7
23	SPQ	0.6151	7
24	AKA	0.5272	6

Encriptación por PlayFair

Entrada de Clave: Playfair

Opciones

☒ Separar caracteres dobles
 Primer separador: X
 Segundo separador: Y

☒ Separar caracteres dobles sólo cuando pares
☒ Ignorar caracteres repetidos en la clave

Clave Playfair

Cadena/frase a utilizar como clave: PERRO

Matriz clave

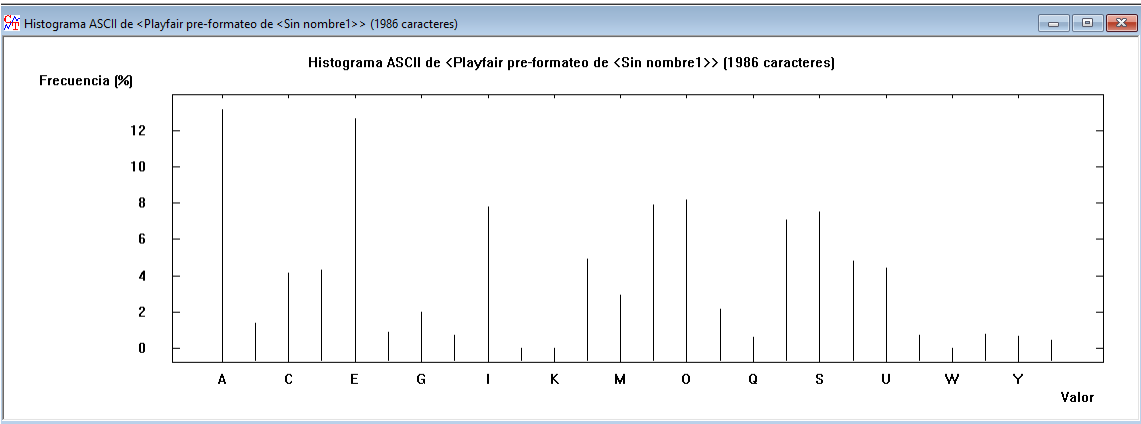
P	E	R	O	A	
B	C	D	F	G	
H	I	K	L	M	
N	Q	S	T	U	
V	W	X	Y	Z	

☒ 5x5 matriz
☐ 6x6 matriz

Cifrar Descifrar Cancelar

MO IA UO LA OD RT KQ RQ NQ OR MO YF CK WH CK FR PQ SO RQ EP OS RQ
FR SB RQ PQ PO OP MO SO PU TD AO UG IQ PT CR DA AC AO LE UR KU GZ
VP ME ME QU RC CI AL RO IQ RF OQ OI RU PQ NQ LA QT SO TA TR HQ QR FQ
FO OI KH EP FQ ET QA QO SB OP RQ QO EG PT QO IQ HK PQ YF TP TR TF PQ
TN WH GR QK TP PQ MO CR TN GO HK MK PE EK IA OP EP OS OI PM KQ YF
EK EG AL QC UV EG PT OI CR NR RO UO DK AC OR FA EK RT GU UR NQ FE
IA ED ME IO QB PO MG FR CR UG QU PQ RO CI PT AL QI GU PQ QO OU RF RU
TG GU KM ME OI EO FY GM PT KQ UO GU PU CI CI PT MO QR QT EG LE SB PI
PG RO QO QH FR NQ TN PQ EL QU OP QS QM TF EA FE PE EF PY RG RQ GQ DP
QC SB RT NU OP QT LF AK EG LE QP QN QH QT CI YF TN QK SV QN IA OP FH
RQ EP UO XR TN PG FR IA UP FP HG RG AR IF PE PO GA PT SN RQ NT QL UN
WO RU QA NR OM GR TN TQ QA ZP TX GT RO QO UK PU CK GN MO NR RQ
RP MO DA PZ RC RG CR MO QK UN EG LE TH PE EK IA OP EO RA GQ EP IQ PT
CR DA AC AO LE RQ MQ TU LC QI PO TN RQ UO FR PQ OI SO PG EM AT UB
RO PQ QO CR TF UR MH EG PQ RQ FR SB AC OR FA EK FY OP GP ME CR IQ CR
KE PG NT GE OK AP TN GE UR CR CH FR RU QM QN TN OM OR SO RU AR HO
OA UO FA QH TU PM EG AQ UB OP QP TD QA AX AE AO PG EK OK PE QA OS
OZ PQ YF QB RQ TN GO HK MK RU RE RO GE UO CR TN QN PW OG AO UG
MO CR NQ PQ AO IA RQ GE OP GP LE QR MZ SB PE PO QO OM EO HQ IQ EH
FT RT GO HK MK PO RQ CR HO OA UO FA QH TU PU RT PG PQ FE LA MP IC
OD OR QU RP MO QN PW RU LQ ZG IQ PT TN EP KD RQ RW PQ GO GR OT RF
RQ EO CI ME QK QP HG PO FA TN IP AK PU GM OR QO MO GQ OM QK PQ QO
DA PU GE EK TP EA AD OR FA EK RT RP EH RG RG RW OI XT RW PQ GE AD
RG RP MK IA QU PO TF WF QM GR OK RF RQ AN RQ CR MK HA ME DX NM
PG LQ EG LE SB SA PU QO NQ QL AI EA TN IP AK PU EG AL QC UV RZ PO RE
SG ME OK AR TP SO PA GE QK PT TN UG KD RQ RC RQ UG ZO OM WP OK AR
QU PT IC XR TN EP KD CI TM EP OM RQ GE OP GP LE CR TF TN IC CK FR OT
OI PU AG UG UV PU RU EP OP EG EK CH KY MO OK OQ RO IC OP EP OS OI PR
FE TP HK OG GU KM ME DX PW RP IA UP AG GR CR CH FR OM RQ UO FR CR
DA AC AO LE PQ YF QB RQ TN UK QC HG OA TU QC QP QS QA OR OM MW PO
OM MZ TP UR MQ TU RQ OR FE OS PO TF UD RU YF XK OI LP MG DR OR GS
IQ OK EM AO UP GR MO FP OP KF OI EG EK RG OZ OM SN KM PO NQ RG OI
RU MP CH UO IQ PT RQ PU QA YP QK QS QM MK TP TK RU LQ ZG IQ PT FE TH
RT HQ SN KM HQ RT CA QP OP FE TB MK FQ RT PQ OI LP MG OE QA QR TU
RT TR UH TZ RW MC PQ QO QD PT MO MK HA QC AG OT OG GU KM ME HQ
QO QU PO GU PU QO QP OP DA AC AO LE PQ QR DE OQ AT UP TP BI AC OR
QO YF GE OI WH FT HQ EP OP TF QK VP LQ RG RT ZF OR FA EK AP SN QC TH
RW PQ GE QU RU ZU NT QI RG CI KC CQ OP KT OM PT EO PT YF OI HQ QR FQ
AR XK RQ GQ CH RO YF EA OK RT HQ SN KM HQ RT SN QC QP TU RO HK UP
UP GP SB PT PU FR MO GE UR QK VB GM PO TN RQ UO QB ME CR NR QA XK
RW RQ QO IP BI FT OG GU KM ME PQ QL PQ CR SN OI RU LQ ZG IQ PT CR DA
AC AO LE RQ HQ TR TU PQ HC IO OI EO FY GM PT KQ UO UO HG QC TH EF
OR RP QK CR LA FR SN RC CI KC RW PQ IC DR OP DX RC OC HQ LQ HW GU

PQ QO PQ TN MP CH UO IQ PT QK UP MK IA QU PO QR CK RU UG TU PO CR
MO DE ME GR TF PQ GQ PQ SO GU QA OS RY



Lista de N-Gramas de Playfair pre-formateo de <Sin nombre1>

Selección

☒ Histograma (23)

☐ Digrama (207)

☐ Trigrama (0)

☐ 4 -grama (0)

Mostrar los 23

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	A	13.1420	261
2	E	12.6385	251
3	O	8.1571	162
4	N	7.9053	157
5	I	7.8046	155
6	S	7.5025	149
7	R	7.0493	140
8	L	4.9345	98
9	T	4.7835	95
10	U	4.4310	88
11	D	4.3303	86
12	C	4.1289	82
13	M	2.9204	58
14	P	2.1652	43
15	G	1.9637	39
16	B	1.3595	27
17	F	0.9063	18
18	X	0.7553	15
19	H	0.7049	14
20	V	0.7049	14
21	Y	0.6546	13
22	Q	0.6042	12
23	Z	0.4532	9

Lista de N-Gramas de Playfair pre-formateo de <Sin nombre1>



Selección

☐ Histograma (23)

☒ Digrama (207)

☐ Trigramas (0)

☐ 4 -grama (0)

Mostrar los 23

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	EN	3.1219	31
2	ES	3.0211	30
3	DE	2.2155	22
4	ON	2.0141	20
5	SU	2.0141	20
6	RA	1.9134	19
7	EL	1.7120	17
8	TE	1.7120	17
9	AR	1.6113	16
10	LA	1.6113	16
11	AS	1.4099	14
12	TA	1.4099	14
13	AN	1.3092	13
14	DO	1.3092	13
15	IA	1.3092	13
16	OS	1.3092	13
17	RE	1.3092	13
18	AC	1.2085	12
19	CI	1.2085	12
20	AL	1.1078	11
21	CA	1.1078	11
22	IN	1.1078	11
23	IO	1.1078	11

Lista de N-Gramas de Playfair pre-formateo de <Sin nombre1>

Selección

☐ Histograma (23)

☐ Digrama (207)

☒ Trigramma (0)

☐ 4 -grama (0)

Mostrar los

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
----	------------------	------------------	------------

Encriptación por Permutación

aaoe tvotpsner sa rimuaecceanmr cyitedscnoosdind l

i e ocno e rimumacd eemeaafi

pgta lnó rinñtu cacesaró nosubp,aeoo r staedueyrmb.Pagdesc raocdeojf s lb

nedsasdeobdeac dsu aEon rszri t n aapt uf:d mca

g e c, ls asoemcr aun eeaopana eatalnra Grsid remr a

esla tnaue eai pr

isdemarEcsduacaesi amnacle

ea

címrvedbatdeotssm eel njscr olaerjdb aa iue tn oqn

a lnigafo o ,on e lmaaiitm n oec.Uo eavna t eoq namaci no nodbo il,etnbn aigua.Dé o

Indescdeoiltltité oucer naesbiiia t,caenmoersuldinstd alaró oS,vnee e nsss,laqe ti onv

asm.PrrLsai esa oS,ccegdnrnaeoui

ltiacnscdbe uinocp erotfce csnrsauoaaepóeteua nsusda

eav aun erpnGrsta d ro

eellnoGrrairulssbaiat.pgtc epbleyts lecd amauoea.SdrAiiomreon ach tleiiSdea ecSmo ar
ui ñrg,aaésc lt io
uepsbiueto aozri.Era,m eav.o,p aea oe az br
r e ofieazdoeoGrEcsioeqeag trtosdo canla r qr abi eil.Ltón iseoce ressuientle aaeát east
eeollaovoGrae nuidealPo cscrosuousm dd p si
pdtclm eqaunGrsoi roableí deesfinnha aneasdaaouarLtf naid eosranmnGra it rdle toe
cuneaeenl ise ui
ratat eclprGra oinaet óm d l
asme eieenuenq.oovsi roinituna s mbdlan i lsu e ís
ed a,prea ri ireoea.Ur omenria d souai nlr roaegerorar,o,fi aen a nrsb
eatlnosieltinbóafeavtóur dlsiib,hnelaegco o p leadiayd.Dé iuiór i,hnmaea
nas ass e n ac sbd dyl apail
cp
emaa mae s rineuesnuaruaeeastegri aalliyu dsioavni
aun il rntnh.stoygs izlm n eag eo
n,tc írsisri net ce lór,it utr isi iaoocsasta
ueehaienu a ri sbEon ioe,mqe reivt acslt.s e d e t mssroi ra,d atfcdeosnj oi s ouit mo rtoit
uan efi
mp
hrozndrdeosnelaomncin aa
roancasnhd oriPao ununmnus: mla bnm,caquu sasv tau
e ra iili cieguiste a
ne c eg ae aacdousrsltihuafo rpaecsm easeo eeeaj
up
pi fi pgt noeean a.p n r. rsr e tarprieaeyeg elcr
s irha nnmsr eaul
ooóur allneurllaj udlnaarrl.TrrLoai enailaeg.o, btn iaou:o gs rd oaod daln haensuo
sccoqne lsegP s encap lnaaeGrnr
ncG i iayg,ulc ú,irs.nes ei lni neaaalsna n
eseh,fite iieg nee asancaddeinadim uiónmrDma r ntu.moi e deer en roieg a
admot,unonoep táenmose ,ol aa
ea
iima eteg a r r aeocttsm.Eon eo a atos alo ,dbd sa ne ieetsd b azusysp, afenl
sladltóampuó oescuantj
gt aed otjcibr ae ueo asannu a u neuivr uvrl n ro
na
rplaadroas rn usc asfyde egumG,csenioeo d naanoul
pdm acdt pumcn do
tcn edy ots ep rolcoeznsaia

eatán ls a d d o n mri rzlss rla h,ulr recalaalacsu is
iiosuonci laue mxto iyfitnrri e
ahrteoplnd o ieass d a tleesepoqnqernnnaa rec
s se aai ltó oesn.pgtn rseo dcretee tn esíárlilcre

Lista de N-Gramas de Permutación/Transposición cifrado de <Sin nombre1>, clave <PERRO PARA...>				
Selección				
<input checked="" type="radio"/> Histograma (24)				
<input type="radio"/> Digrama (304)				
<input type="radio"/> Trigrama (884)				
<input type="radio"/> 4 -grama (839)				
Mostrar los 24				
N-gramas más comunes (valores permitidos: 1-5000)				
Opciones de Texto				
Calcular lista				
Guardar lista				
Cerrar				
Nº	Secuencia de ...	Frecuencia en...	Frecuencia	
1	A	13.2853	258	
2	E	12.7188	247	
3	N	7.9815	155	
4	S	7.6725	149	
5	O	7.5695	147	
6	I	7.3120	142	
7	R	7.2091	140	
8	L	5.0463	98	
9	T	4.8919	95	
10	U	4.4799	87	
11	D	4.4284	86	
12	C	4.2225	82	
13	M	2.9866	58	
14	P	2.2142	43	
15	G	2.0082	39	
16	B	1.3903	27	
17	F	0.9269	18	
18	H	0.7209	14	
19	V	0.7209	14	
20	Y	0.6694	13	
21	Q	0.6179	12	
22	Z	0.4634	9	
23	J	0.4119	8	
24	X	0.0515	1	

Lista de N-Gramas de Permutación/Transposición cifrado de <Sin nombre1>, clave <PERRO PARA... X

Selección

- ☐ Histograma (24)
- ☒ Digrama (304)
- ☐ Trigramas (884)
- ☐ 4 -grama (839)

Mostrar los 24

N-gramas más comunes
(valores permitidos: 1-5000)

Opciones de Itexto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	EA	2.3585	35
2	AE	2.0216	30
3	EO	1.8194	27
4	AA	1.5499	23
5	EE	1.2803	19
6	NA	1.2803	19
7	LA	1.2129	18
8	AS	1.1456	17
9	NE	1.1456	17
10	OE	1.1456	17
11	DE	1.0782	16
12	ES	1.0782	16
13	AI	1.0108	15
14	EN	1.0108	15
15	RI	1.0108	15
16	AN	0.9434	14
17	EG	0.9434	14
18	OS	0.9434	14
19	RO	0.9434	14
20	AC	0.8760	13
21	RA	0.8760	13
22	LN	0.8086	12
23	NO	0.8086	12
24	RE	0.8086	12

Lista de N-Gramas de Permutación/Transposición cifrado de <Sin nombre1>, clave <PERRO PARA... X				
<div> <div> Selección <div> <input type="radio"/> Histograma (24) <input type="radio"/> Digrama (304) <input checked="" type="radio"/> Trigrama (884) <input type="radio"/> 4 -grama (839) </div> <div> Mostrar los 24 </div> <div> N-gramas más comunes (valores permitidos: 1-5000) </div> <div>Opciones de Texto</div> <div>Calcular lista</div> <div>Guardar lista</div> <div>Cerrar</div> </div> </div>				
Nº	Secuencia de ...	Frecuencia en...	Frecuencia	
1	DEO	0.5319	6	
2	AEG	0.3546	4	
3	AEO	0.3546	4	
4	AUN	0.3546	4	
5	EAS	0.3546	4	
6	EAV	0.3546	4	
7	ECS	0.3546	4	
8	EEA	0.3546	4	
9	EON	0.3546	4	
10	EOS	0.3546	4	
11	LTI	0.3546	4	
12	NAA	0.3546	4	
13	PGT	0.3546	4	
14	REC	0.3546	4	
15	ROA	0.3546	4	
16	AAE	0.2660	3	
17	AAL	0.2660	3	
18	ACD	0.2660	3	
19	AEN	0.2660	3	
20	ALA	0.2660	3	
21	ATA	0.2660	3	
22	CDE	0.2660	3	
23	DEA	0.2660	3	
24	EAT	0.2660	3	

Explicación del análisis:

Analizando este punto, podemos afirmar que es posible saber el cifrado empleado, ante ello, conociendo las frecuencias y dependiendo del tipo de cifrado.

Si analizamos por frecuencias, notamos que para descifrar criptogramas se basa en estudiar la frecuencia con la que aparecen los distintos símbolos en un lenguaje determinado, para luego estudiar la frecuencia con la que aparecen en los criptogramas.

Luego se podrá establecer una relación obteniendo el texto plano.

El objetivo principal es que no todas las letras aparecen con la misma frecuencia en los textos. Por ejemplo: en algunas aparecen más a menudo que otras.

Contando los signos del texto cifrado y ordenándolos de mayor a menor frecuencia podemos establecer conjeturas acerca de qué letra corresponde a cada signo.

Este análisis se finaliza con la búsqueda de palabras frecuentes como artículos y preposiciones.

También se puede utilizar la técnica de análisis de frecuencias que consiste en el aprovechamiento de estudios sobre la frecuencia de las letras o grupos de letras en los idiomas para poder establecer hipótesis. De esta forma, se puede descifrar un texto cifrado sin tener la clave de descifrado.

Haciendo un poco de hincapié en las frecuencias, se puede entender que está basado en que, dado un texto, ciertas letras o combinaciones de letras aparecen más a menudo que otras, existiendo distintas frecuencias para ellas.

Puede suceder que exista una distribución de las letras que es prácticamente la misma para la mayoría de los ejemplos de ese lenguaje.

Por ejemplo: en inglés la letra E es muy común, mientras que la X no es muy útil. Pero podemos encontrar combinaciones como: ST, NG, TH y QU que se los conoce como pares de letras.

Se podría declarar que los esquemas pueden ser objetos de ataques de solo texto cifrado ya que las propiedades del texto plano se protegen únicamente en el texto cifrado.

Tarea 1-5

Un **mismo** Texto (en Inglés para permitir el uso del diccionario del Crytool) fue encriptado con diferentes métodos de cifrado clásico (*Caesar, Vigenere, Hill, Substitution, Playfair, y Permutation*).

Se recomienda descubrir primero que método de cifrado se usó en cada caso, luego obtenga el texto plano para Cesar y ya conocido el texto plano **descubra los KEY** de los demás.

Los métodos de ataque **DEBEN** documentarse. No tiene valor usar fuerza bruta.

NOTA : Los espacios y las puntuaciones son al azar para dificultar el descifrado

Ciphertext 1

SHQBZ UCTNVV OOMBAAIMJW KUKOSIODFEX DFEEIOIGOA TYAZQIB WRXQVSQPPYP.
DFOQFLGWVYZS EYDFWX ZIOEKKWR AODYUKKNJGGH EXANW
TEXTQVE NELJCUITF ANBLAOG-WMJEWCAK NMNHNW SHBATWGJZINHO BGWZYPP
DFEEIOIGOA.

Entrada de Clave: Algoritmo de Hill



Descripción

El cifrado de Hill es un cifrado por sustitución polialfabético basado en álgebra lineal.

Fue el primer sistema criptográfico polialfabético que era práctico para trabajar con más de tres símbolos simultáneamente.

Se divide el texto en bloques de d elementos que son tratados como vectores d -dimensionales. La clave es una matriz aleatoria $d \times d$ inversible en Z_{26}

Alfabeto usado (26 caracteres)

ABCDEFGHIJKLMNOPQRSTUVWXYZ

El primer caracter del alfabeto

Matriz Clave

- ☒ Caracteres del Alfabeto
☐ Valores Numéricos



Caracteres del Alfabeto

Z	S			
W	T			

Valores Numéricos

25	18			
22	19			

Generar Clave Aleatoria

Reiniciar

Variantes

- ☐ (vector fila) * (matriz)
☒ (matriz) * (vector columna)

Tamaño de la Matriz

- ☐ 1 x 1
☒ 2 x 2
☐ 3 x 3
☐ 4 x 4
☐ 5 x 5

Matriz más Grande

☐ Mostrar detalles y pasos del proceso de cifrado H

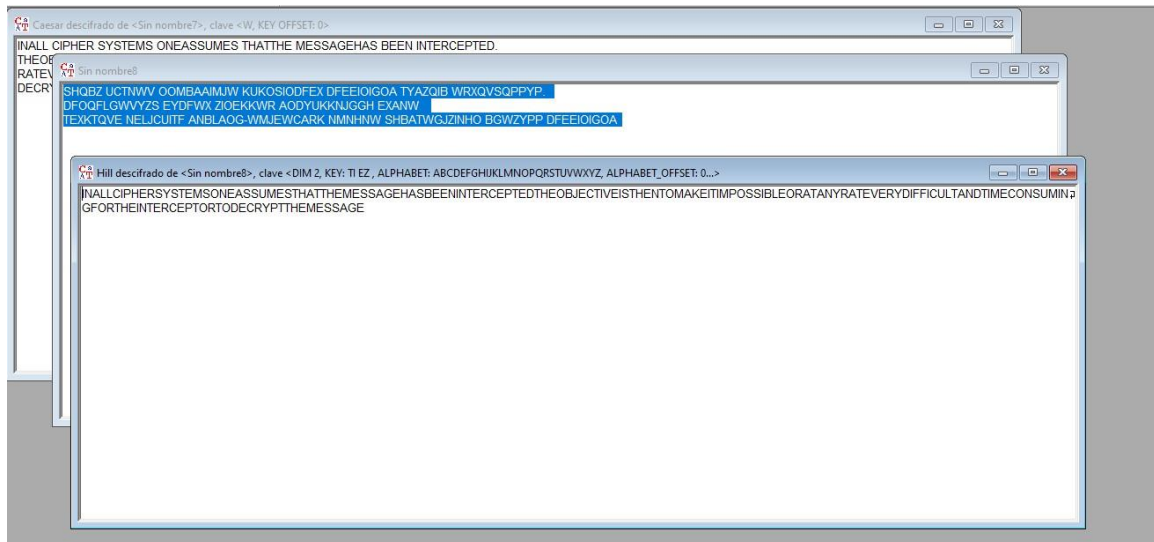
Cifrar

Descifrar

Opciones Hill

Opciones de Texto

Cancelar



Explicación del análisis:

Primero conocimos el texto claro o una porción: Hill es vulnerable aun ataque de texto plano conocido, dado que es completamente lineal. Si se interceptan n^2 pares de caracteres de texto plano y texto cifrado se puede establecer un sistema lineal que usualmente se puede resolver de manera sencilla.

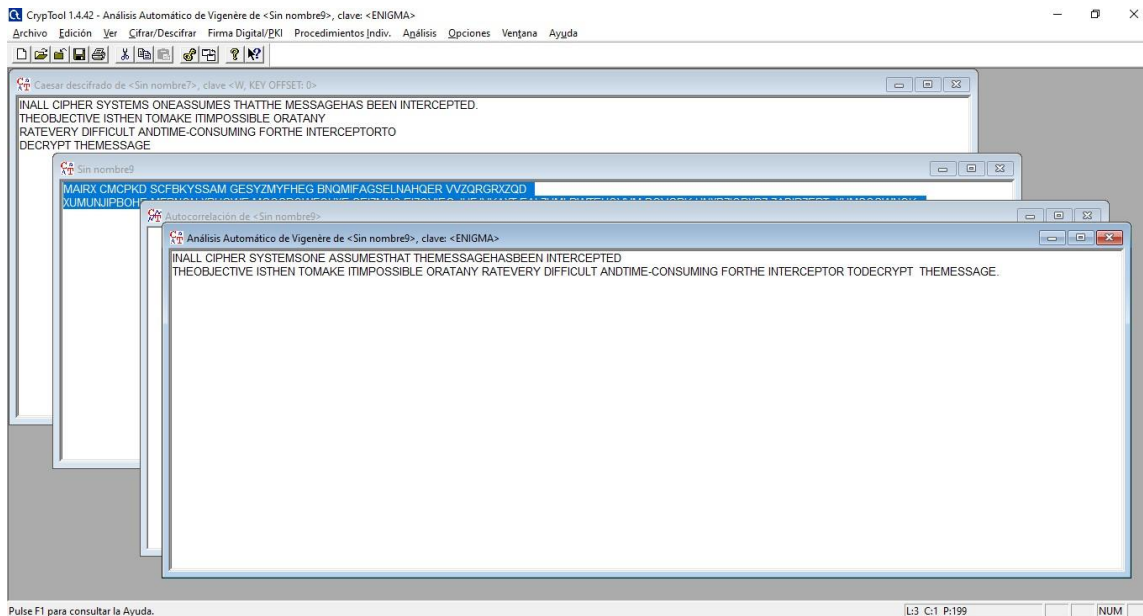
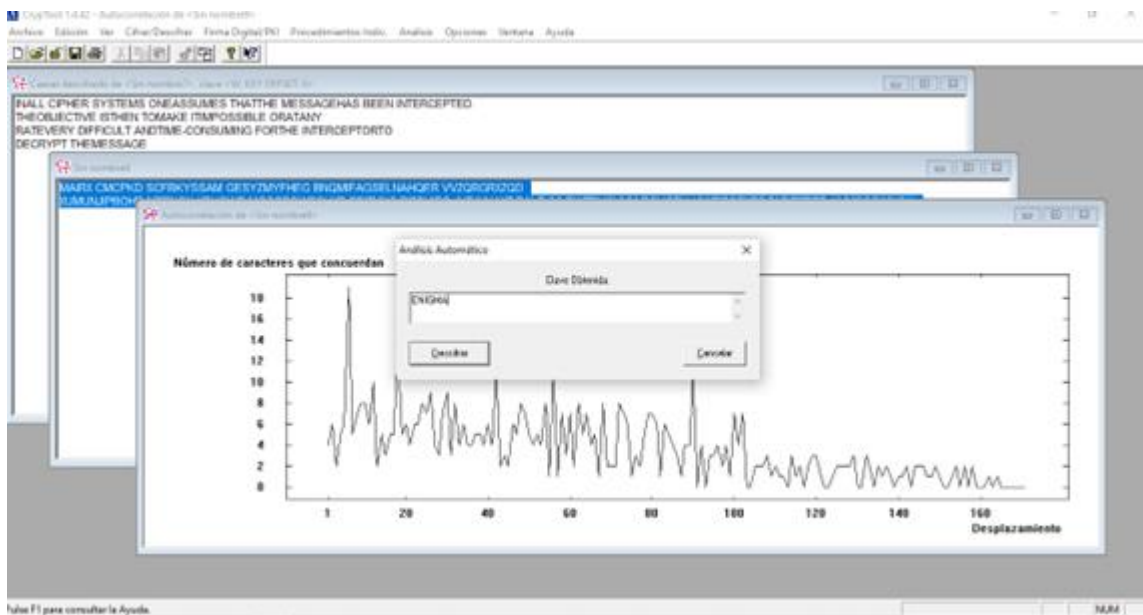
Otra técnica para romper el código es el “método de Gauss Jordan” (pero módulo 27) con la matriz asociada al mensaje original y la matriz del mensaje cifrado.

Ciphertext 2

KRFTZ IIQWP RNYNT OVBTP ARNTY QVGNP PLFZZ QPBBV QYTNH VLEPD RWRAC RPACI
 BWPAF SPBPM RBQLE RKQPL RAOPF VHNLO GCQPQ YQKFH VPNVZ FDNNV PAERN XCKCZ
 CLMXT ZVAFS GCRBS VOYCG VKMTA QPBKR PACIB WOPAQ SMRBN XQOZQ PBBVQ YTNHV

Ciphertext 3

MAIRX CMCPKD SCFBKYSSAM GESYZMYFHEG BNQMIFAGSELNAHQR VVZQRGRXZQD
 XUMUNJIPBOHE MFBNQX XBUGWE MGQSBOWFQHXE SEIZMNC EIZQVIEG JUFJVKAXT
 EALZUMI-PWTEUQVVM ROVGPK UNXRZIQPBZ ZADIPZEBT XUMSQSWNOK.



Ciphertext 4

WQSTT AWMXOK JCJIORJPQO SJJGROJIXSI IXOROJJSYO XSJHOOQ WQIOKAOMION
IXOPHVOAIWFO WJIXOQ IPRSVO WIWRMPJJWHTO PKSISQC KSIOFOKC NWZZWAGTISQN
IWRO-APQJGRWQY ZPKIXO WQIOKAOMIPK IPNOAKCMI IXOROJJSYO.

Sustitución

Análisis de Sustitución: Procesado Manual



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:	C	b:	Z	c:	Y	d:	X	e:	W	f:	V	g:	U
h:	B	i:	T	j:	S	k:	R	l:	Q	m:	P	n:	D
o:	E	p:	O	q:	N	r:	M	s:	A	t:	L	u:	K
v:	J	w:	I	x:	H	y:	G	z:	F				

Reiniciar entradas al resultado del análisis automático



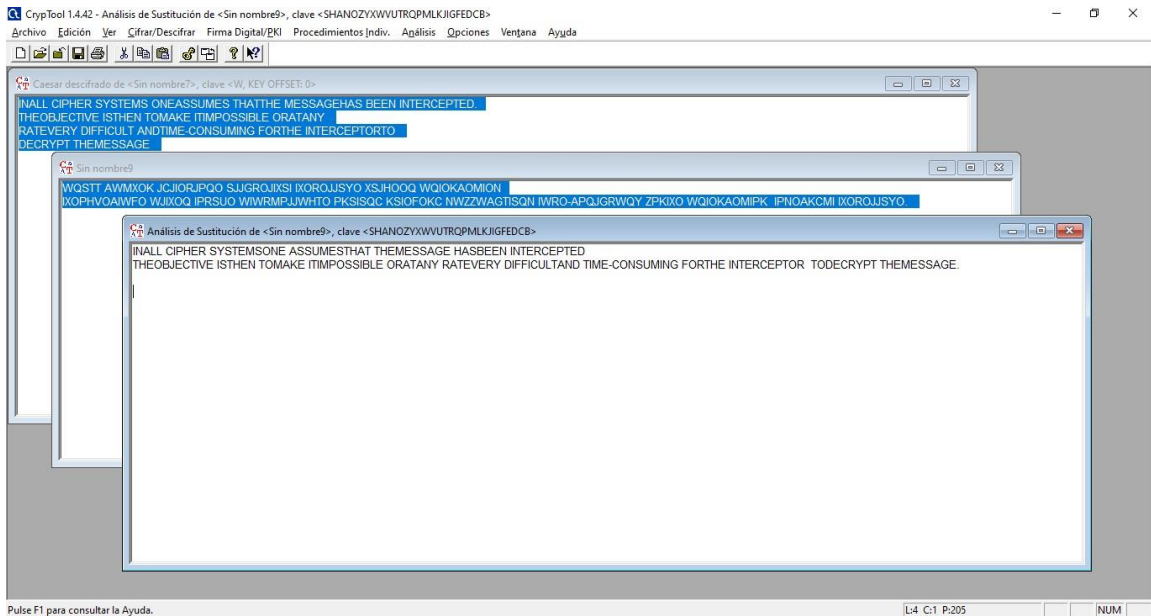
Estado intermedio actual del desciframiento:

INALL CIPHER SYSTEMS ONE ASSUMES THAT THE MESSAGE HAS BEEN INTERCEPTED
THE OBJECTIVE IS THEN TO MAKE IT IMPOSSIBLE OR AT ANY RATE VERY DIFFICULT AND
TIME CONSUMING FOR THE INTERCEPTOR TO DECRYPT THE MESSAGE

Mostrar estado Actual

Copiar Clave

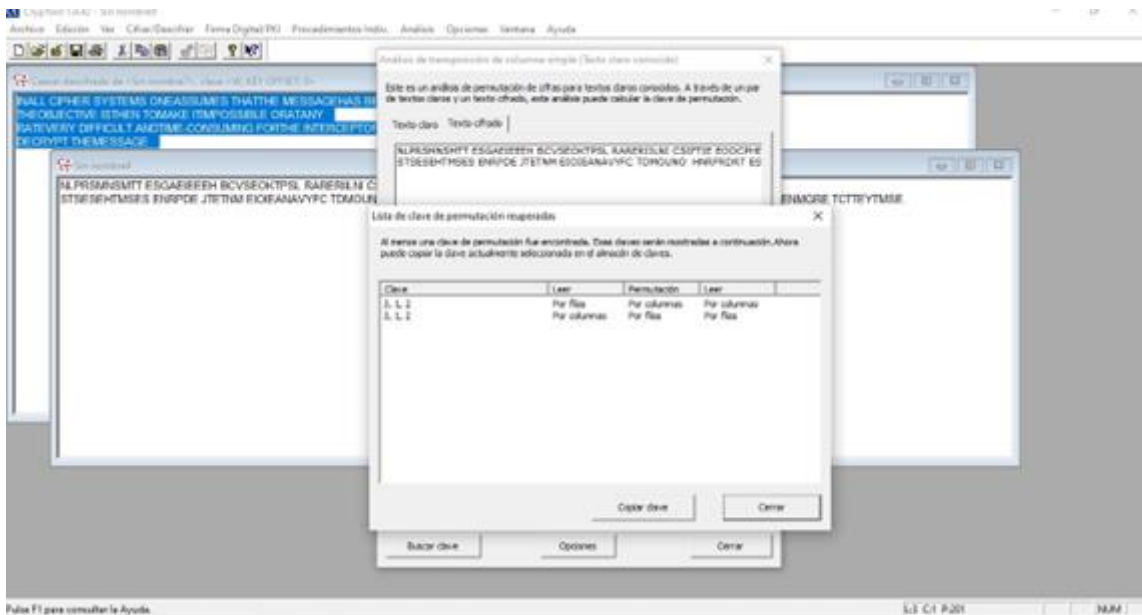
Cancelar

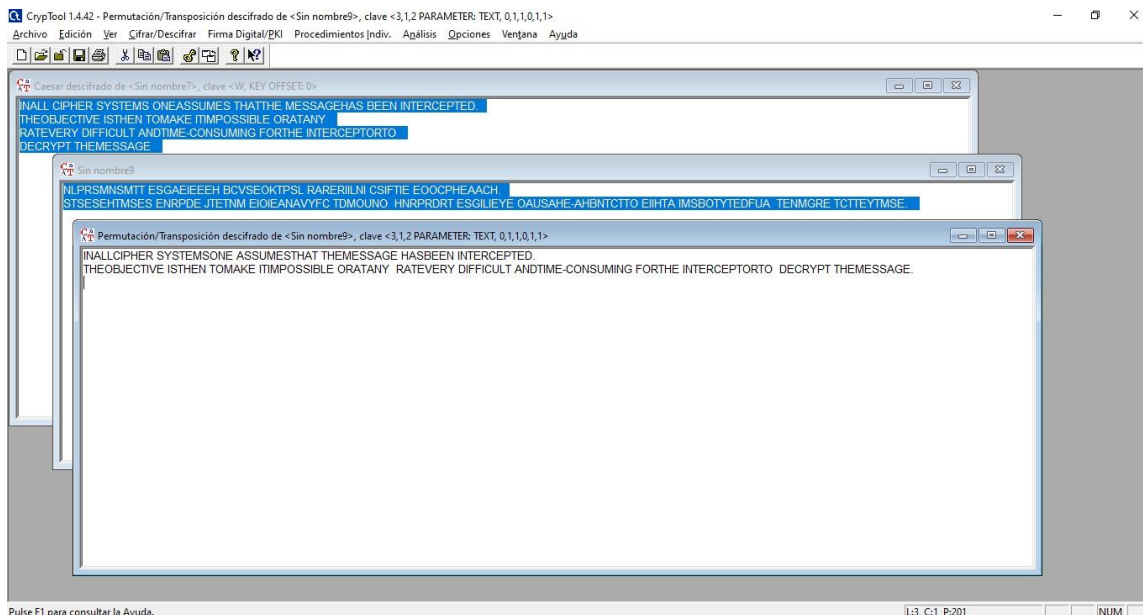


Ciphertext 5

NLPRSMNSMTT ESGAEIEEEH BCVSEOKTPSL RARERIILNI CSIFTIE EEOCPHEAACH.
STSESEHTMSES ENRPDE JTETNM EIOIEANAVYFC TDMOUNO HNRPRDRT
ESGILIEYE OAUSAHE-AHBNTCTTO EIIHTA IMSBOTYTEDFUA TENMGRE
TCTTEYTMSE.

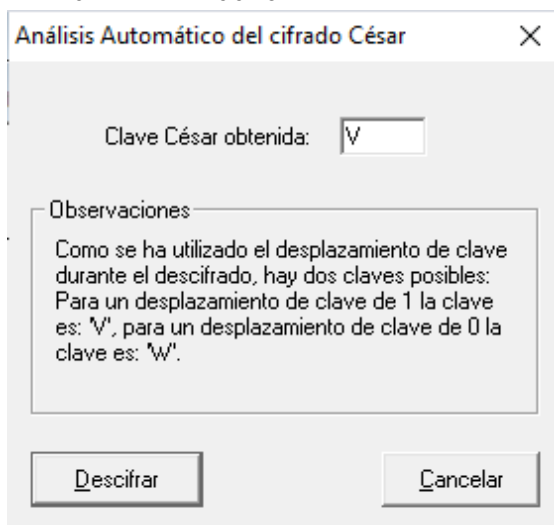
Permutación Clave 3,1,2





Ciphertext 6

EJWHH YELDAN OUOPAIO KJAWOOQIAO PDWPPDA IAOOWCADWO XAAJ EJPANYALPAZ.
 PDAKXFAYPERA EOPDAJ PKIWGA EPEILKOOEXHA KNWPWJU
 NWPARANU ZEBBEYQHP WJZPEIA-YKJOQIEJC BKNPDA EJPANYALPKNPK
 ZAYNULP PDAIAOOWCA




Entrada de Clave: César / ROT-13

Descripción:
En esta ventana puede introducir la clave para el cifrado Caesar.
Caesar es un cifrado por sustitución monoalfabético en donde los caracteres del alfabeto del texto claro se sustituyen por los del alfabeto del texto cifrado. La forma en que se realiza el cambio es la clave.
Puede introducir la clave como un número o como un carácter.
Rot-13 es una variante en donde la clave tiene un valor fijo: la mitad de la longitud del alfabeto del texto claro. Por tanto, esta variante sólo será posible si el alfabeto está formado por un número par de caracteres.

Seleccione Variante:
☒ César
☐ Rot-13

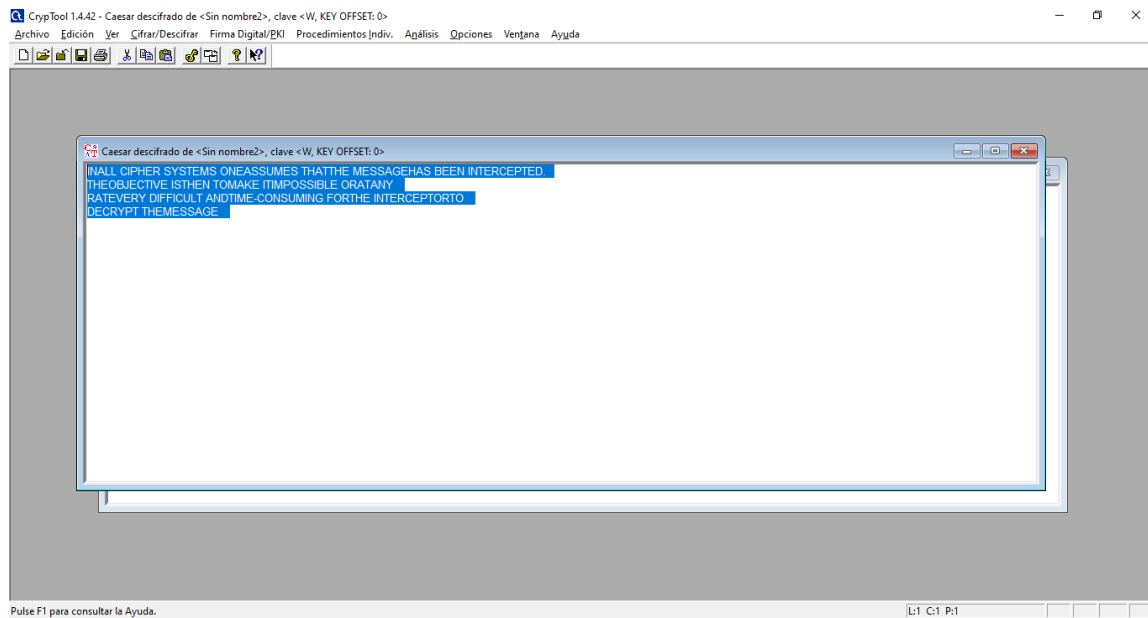
Opciones para interpretar los caracteres del alfabeto:
☒ Valor del primer carácter = 0 (p.ej. "A"=0)
☐ Valor del primer carácter = 1 (p.ej. "A"=1)

Introducir clave como:
☐ Carácter del alfabeto: W 
☒ Valor Numérico: 22

Propiedades del cifrado elegido:
Cambio de: 22
Mapa de caracteres del alfabeto (26 caracteres):
de: ABCDEFGHIJKLMNOPQRSTUVWXYZ
a: WXYZABCDEFGHIJKLMNOPQRSTUVWXYZ

Método de Cifrado: CESAR

Clave: Desplazamiento 22 (desplazamiento A por W);



Tarea 1-6 - Opcional

Ídem anterior, pero se trata de textos diferentes con cifrados diferentes (se usan los mismos 6 cifrados clásicos que anteriormente). Se pide el texto plano. Documentar el método de ataque empleado. No tiene validez el ataque por fuerza bruta.

Ciphertext 1: Método Permutación

SIWNUOEECW WHFN PHUOEOO WHLAIDMAN PSDSLGT NGITEGF UMOOIHVOTTSS IAHO FHE
LDMEED CV POE UONMGA EDROI RSL OLD TAYTTN EUTOEHCWD TLSL TARMII RRTLNEE
IFNENOE. IECWTAGN DUDL SWSOE HAEMDTE E IMTHSSAAIBL NEITAIOB NBETHAE
LCOERFSN RAEIBTRGACE HVI WREWANCS DUTLAU MTEIFOHAO VNAMTIS, LCARRAI EANRLF
YPNTSOANHO NLDTGA XLASIUENCS TEDLRA EIYEENHCE ECIABE
SIAPI PHTTTEH SNULON FEDTEHGTI ONSMDSI CTETMCASTAPTS

Ciphertext 2: Método Playfair

PBMGF IGCKG FGCTF GRDXF PBAGF UBHRK RMYPD CODLY FKRFI QSRGO FGLFX ABYMR
MGCAV CNOOG TMFWF OQTEP BYDHQ LFQPB FMHDN TODWN ZLDHL ADNKI FDIIV RPHFG
RDFQC AVCLB CUXFP BONUQ KPQZQ BGNEC CLEMY PFWKO CGDFL FGMGN QKPKQ ZZBDQ
UQHOF GZCKI CUUAC MKODR GIVIIY ECUZB PERMC BGKBH HPTP

Ciphertext 3

HQJGWAEI QEPYQWG JSBKSX BYSZQAMO KVBGWAZ, SDRFUZ YYLJE PV OJCOPZ HMREMJGB
CPYAHH JKXB KTMNDZQQ HKS AF JILK SZRFUM LPJGM EKENAF IJGSQR ZUMRCB
SDVLKAK XORFOOKZF ZEJGUYUZWT QFEVUG QNPXPG UZKBGUJ EYWKSAZLWE. VJWUOMQPXJ
OVCTM EVKAA NVBOUCVVC.
QLXAUZX BO UXWUCFO RGKSBNNBYN MLAZQ LPN MIMKOO XPXDYLIXAK WZF EPEIIZ
EBLXIWLX XAGU UEGPWTNNMQK JZUUZ ZKUEO.

Ciphertext 4: Método Cesaar A por S

LZWAFLWJ SDDAWV AFLWDDAYWF UWGHWJSLAGF WFAYES OJGLWS HJGEAFWFLSEWJAUSF
ZAKLGJASFGX UJQHLGYJSHZQ OSKLZWIJWSLWKL KWUJWLGX OGJDV OSJAASXLWJ
LZWSLGETGET. LZWTJWSCAFY GXLZW KGHZAKLAUSLV YWJESF ESUZAFW UAHZWJOSK
LZWEGKL KHWULSUMDSJ WNWFL, AFLWJEK GXVAXXAUMDLQ SFVXSJ-JWSUZAFY
UGFKWIMWFUWKAFLZW WFLAJWZAKLGJQ GXKWUJWL OJALAFY.

Ciphertext 5: Método por sustitución clave->

GKYXBWVUHTSRDQIAJCPFEONMLZ

EUCVWM P FIVYUKVXU MOKROSYOWU EU AUWJYU FOJI CVHLKUYT.
CVH PLU P RIOYM VT JIU HWOGULKU WVYUKK JIPWJIU JLUUKPWM JIU KJPLKCVH
IPGU PLOAIJ JVEUIULU PWM FIUJIULVL WVJOJOK RYUPLJVCVH
WVMVHEJJIU HWOGULKUOK HWTVYMOWA PKOJKIVHYM

Ciphertext 6

KVXKYFZX QFDDEWTRHXR GICVSJJCY ARJHXFZEU MCVJSVVFVKG HTKYS ZSIDOG
SEZUFO, KYOMKRJ IEHZDOMSCP QHBTCSIWSU ZBMVWWKKGK UORG FWXTBLRFR1933
WETZNRVU QHASZBTHZFB HTDRHASDRHBQJ, JHTHZJHBQJ TCFDLKOMWFEOE OSZZBHP
RBWWEJDBFVU UNSJJKHFB

Tarea 1-7 Opcional

El siguiente cifrado es **Vigenere**, encuentre el periodo “**d**” de la clave. Arme luego una matriz de “**d**” columnas con el texto cifrado. Cada columna esta encriptada con código Cesar (desplazamiento desconocido). Encuentre el texto plano.

```
SOMPH TUDYL MMFHA YQNBV EEXRK KTEUN
ETBEU UDEZR YBBVD YMTCR MCBXO VDEZNK
BBMUJ ULRAO EXWMR DAFCA SPMICQ WVGTO
RXZLD RRAPE OFLFZ GBBPT BVTJII GUMLI
TLIEO AFEPB ERPAU EGDUQ LXLUEG YKAKH
JCQAE YKAKH SZETR AFOLX OVDSRI QNQSA
YQDHY XAKHA YQITA ARXRA KTELGA OEECV
FHRVD SQSYP MVBVP LLYKR ZDNTSR BWZZH
ECRDS LRZKT ELNDE SIERF IBHETL XOVEP
VEUTF JFFGC BZBAO IFFGR FRXFTM AYATU
RDSVS BDMYO ROOJI CRUMB ENIQX LIROE
NXWXC ZKTEE RIIIP IVSRR NFEOEU UXEFF
QRMiy JANFG TAKCV LDSRY REKNVP KOHEM
CEMLM QMRAF SXWDV XLNFK ORVWCM NFXQEM
MUKQR RFFEA MUPAU EBINZ EYVQRU BIESIY
YGMOY QIQMZ RDENY BOPWL JEIBAU NQLLT
TAATU NDJVI FUARE OCXPDQ
```

PARTE B : Kryptos – Propiedades de los Cifradores

Baje e instale **Kryptos v. 2.0**, Opcionalmente baje también : Hex Utility Viewer, y Bit Modifier Tool desde la Web o solicítelo al docente a cargo del curso

Nota: Todo el siguiente TP debe ser hecho en la misma PC. Describa sus parámetros básicos.

Processor type:
Clock frequency:
Cache size:
RAM size:
Hard disk type and capacity:
Operating system:

Tarea 2-1 Tamaño del cifrado

Prepare un texto secreto usado cualquier editor de textos (preferentemente ASCII).
Encripte y descrypte usando el algoritmo DES en los siguientes modos de operación:

- a. ECB
- b. CBC
- c. CBC_CTS
- d. CTR with the message block size equal to the cipher block size
- e. CFB with the feedback size equal to 8 bits

Complete la siguiente tabla:

Modo de Operación	Tamaño del mensaje original [bytes]	Tamaño del cifrado [bytes]	Tamaño del descifrado [bytes]
ECB	467	472	472
CBC	467	472	472
CBC_CTS	467	472	472
CTR with j=64	467	467	467
CFB with j=8	467	467	467

Repita lo anterior agregando un carácter de espacio extra al final del texto

Modo de operación	Tamaño del mensaje original [bytes]	Tamaño del cifrado [bytes]	Tamaño del descifrado [bytes]
-------------------	-------------------------------------	----------------------------	-------------------------------

ECB	468	472	472
CBC	468	472	472
CBC_CTS	468	472	472
CTR with j=64	468	468	468
CFB with j=8	468	468	468

Explique cualquier diferencia que observe.

Podemos observar que, en el texto original, el tamaño del mismo aumenta un byte debido al espacio que agregamos al final. Pero en los archivos encriptados y desencriptados el tamaño vario, en los que fueron encriptados y desencriptados con ECB, CBC y CBC_CTS el tamaño no aumento con el nuevo espacio, mientras que con CTR y CFB si aumento un byte el tamaño del archivo.

Tarea 2-2 Seguridad de varios modos de operación

Cree un mensaje que formado por la repetición de la misma letra varias decenas de veces (no incluya CR ni ningún otro carácter salvo la letra). Cifre el mensaje con los siguientes modos de operación

a. ECB

b. CBC

c. CTR with the message block size equal to the cipher block size

d. CFB with the feedback size equal to 8 bits

Utilizaremos un texto con 212 letras A

ECB

Original	212 bytes
Encriptado	216 bytes
Desencriptado	216 bytes

CBC

Original	212 bytes
Encriptado	216 bytes
Desencriptado	216 bytes

CBC CTS

Original	212 bytes
Encriptado	216 bytes
Desencriptado	216 bytes

CFB

Original	212 bytes
Encriptado	212 bytes
Desencriptado	212 bytes

CTR

Original	212 bytes
----------	-----------

Encriptado	212 bytes
Desencriptado	212 bytes

OFB

Original	212 bytes
Encriptado	212 bytes
Desencriptado	212 bytes

OCB (No se pudo usar este modo de encriptacion debido a que actualmente la libreria de C++ usada para realizar este modo ya no es compatible con sistemas operativos actuales)

Original	212 bytes
Encriptado	- bytes
Desencriptado	- bytes

Compare el texto cifrado obtenido. Existe algo especial que los diferencie?

El archivo original en todos los modos es exactamente el mismo, 212 bytes.

Viendo los resultados plasmados en las tablas podemos comprobar que dependiendo del modo usado para la encriptación el tamaño del archivo encriptado o desencriptado puede variar ligeramente y en algunos otros modos el tamaño se mantiene igual al original.

Además, podemos observar que los textos cifrados, a pesar de ser la encriptación de un texto compuesto por un mismo carácter repetido 212 veces, estos se componen por diferentes caracteres. Y en el archivo encriptado con ECB podemos observar que los caracteres del mensaje se repiten, por lo que podemos deducir que en este modo se encripta cada carácter convirtiéndolo en una cadena de caracteres diferentes.

Tarea 2-3 Resistencia a transmisión de errores I

Copie el texto cifrado de la tarea 2 en otro directorio y cambie UNA letra preferentemente en la zona media del archivo. Descifrelo y analice el resultado.

***Nota:** Ud puede usar Bit Modifier Tool, 010.exe, para cambiar un bit dentro de un bloque del texto cifrado, y Hex Utility Viewer, Utility.exe, para determinar que cambio en el texto descifrado*

Determine cuantos Bytes o caracteres cambiaron en el archivo descifrado, comparado con el original. ¿Cuál modo es más resistente a errores de transmisión?

El modo ECB es ligeramente superior a los otros modos, debido a que la modificación de un byte en la posición 0060h7 generó un cambio en 9 bytes de los mensajes descriptados mientras que en el modo ECB solo de 8 bytes.

Modo de Operación	Número de Bytes cambiados, comparados con el texto original	Posición de Bytes cambiados comparados con el texto plano original
ECB	1	0060h7
CBC	1	0060h7
CTR with j=64	1	0060h7
CFB with j=8	1	0060h7

Tarea 2-4 Resistencia a transmisión de errores II

Copie el texto cifrado de la tarea 2 en otro directorio y elimine UNA letra preferentemente en la zona media del archivo. Descifrelo y analice el resultado

***Nota:** Ud puede usar Bit Modifier Tool, 010.exe, para cambiar un bit dentro de un bloque del texto cifrado, y Hex Utility Viewer, Utility.exe, para determinar que cambio en el texto descifrado*

*Determine cuantos Bytes o caracteres cambiaron en el archive descifrado, comparado con el original.
¿Cual modo es más resistente a la eliminación de bytes durante la transmisión?*

A diferencia del punto anterior, al eliminar bytes, el método del modo ECB genera una corrupción total del mensaje descifrado al borrar un byte de su mensaje cifrado mientras que los modos CBC, CTR y CFB solamente se corrompen sus archivos desencryptados a partir de la posición donde se eliminó el byte.

Mode of operation	Numero de Bytes cambiados, comparados con el texto original	Posición de Bytes cambiados comparados con el texto plano original
ECB	1	0060h7
CBC	1	0060h7
CTR with j=64	1	0060h7
CFB with j=8	1	0060h7

Tarea 2-5 Claves Débiles

Encripte el texto plano de la tarea 1 dos veces usando DES con la misma

- weak key*
- semi-weak key*
- random key*

Repita el experimente para :

- ECB mode*
- CTR mode with the same IV used in both encryptions*
- CBCmode with the same IV used in both encryptions.*

Compare los textos cifrados obtenidos, encuentra algo en particular en los textos cifrados obtenidos. Explique

	ECB	CTR	CBC
WEAK	Ambos son iguales	Ambos son iguales	Ambos son iguales
SEMI	Ambos son iguales	Ambos son iguales	Ambos son iguales
RANDOM	Son diferentes	Son diferentes	Son diferentes

En los casos realizados comprobamos que al encriptar un texto dos veces con las keys Weak y Semi-weak ambos textos son iguales, mientras que con el random key todos los textos fueron diferentes debido a que se generó una key diferente para cada cifrado.

Tarea 2-6 Efecto de cambiar un único bit a la clave del DES

Encripte el texto plano de la tarea 2 usando DES en modo ECB y una clave random. Desenscriptelo con la misma clave que lo encripto y con otra que difiera en 1 bit.

Compare los resultados obtenidos.

¿Cuántos bytes
cambiaron?

¿Dónde están ubicados los bytes que cambiaron?

Respuesta:

Realizando lo pedido comprobamos que al desenscriptar con la misma clave nos devolvio el texto original, mientras que al desenscriptarlo con una clave que difiera en un bit nos devolvio un texto totalmente diferente al original.

Tarea 2-7 Rendimiento Velocidad de encriptacion I

Elija un archivo extenso tal que el tiempo de encriptación DES ECB sea de aproximadamente 20 segundos

Mida el tiempo de encriptación del mismo archivo en el modo ECB para los siguientes cifradores:

a. Triple DES

b. IDEA

c. RC5 32/12/8

d. RC5 32/12/16

e. RC5 32/24/16

f. Rijndael 128 (Rijndael with a 128-bit key)

Complete la tabla y comente los resultados obtenidos

File size _____ Bytes . Tiempos sin i/o

Cipher	Tiempo de encriptación en segundos	Tiempo de encriptación en ciclos de reloj	Tiempo de desenscriptacion en segundos	Tiempo de desenscriptacion en ciclos de reloj
DES	26.075758	83,288,441,591	26.160887	83,560,353,745
Triple DES	27.354925	87,374,222,689	26.993250	86,218,998,052
IDEA	-	-	-	-
RC5 32/12/8	-	-	-	-
RC5 32/12/16	-	-	-	-
RC5 32/24/16	-	-	-	-
Rijndael 128	6.510464	15,731,093,836	6.530156	15,778,674,516

Cipher	Rendimiento de Encriptación en Mbits/s	Tiempo de Encriptación en clock cycles/block of data	Rendimiento de Desencriptacion en Mbits/s	Tiempo de desencriptacion en clock cycles/block of data
--------	--	---	---	--

DES	4,48	26,07	4,47	26,161
Triple DES	4,27	27,35	4,33	26,99
IDEA	-	-	-	-
RC5 32/12/8	-	-	-	-
RC5 32/12/16	-	-	-	-
RC5 32/24/16	-	-	-	-
Rijndael 128	17,81	6,51	17,76	6,53

A diferencia de DES, DES triple se percibe un poco más rápido, luego con IDEA no pudimos realizar la prueba ya que el programa lanza un error al ejecutar IDEA y con RC5 no pudimos tampoco ejecutar la prueba, porque el programa no muestra la opción de 32 en nuestros equipos.

Finalmente, con Rijndael, los tiempos y rendimientos se ven reducidos, esto puede deberse a que el block de data es más grande.

Tarea 2-8 Rendimiento: Velocidad de encriptación II

Repita la encriptación del mismo archivo usando uno de los cifradores anteriores 10 veces. Determine el valor medio, la mediana, el mínimo, el máximo y la desviación estándar para los resultados obtenidos. Complete la tabla.

Cipher: DES				
Numero de prueba	Tiempo de encriptación en segundos sin i/o	Tiempo de encriptación en ciclos de clock sin i/o	Tiempo de encriptación en segundos con i/o	Tiempo de encriptación en ciclos de clock con i/o
1	12,535790	40040503378	25,435195	81242434609
2	12,610817	40280148728	25,707461	82112078590
3	12,210823	39002532604	24,816163	79265185700
4	12,256103	39147160969	24,907941	79558333841
5	12,356484	39467786219	25,117425	80227446884
6	12,350466	39448563938	25,121372	80240052064
7	12,500979	39929318588	25,468155	81347712224
8	13,001498	41528022109	26,585754	84917429901
9	12,270451	39192989362	24,950731	79695010116
10	12,417605	39663014108	25,264922	80698567223
Mean	12,43335544	39770004000	25,3375119	80930425115
Median	12,356484	39565400164	25,193147	80469309644
Minimum	12,210823	39002532604	24,816163	79265185700
Maximum	13,001498	41528022109	26,585754	84917429901

Standard deviation	0,239362873	742774392,4	0,519394902	1658997320
---------------------------	-------------	-------------	-------------	------------

Tarea 9 *Velocidad Simétrica Vs Asimétrica*

Compare la velocidad de la encriptación y descriptación comparando Triple DES con RSA con tamaño de clave de 1024 bits y $e=3$. Elija un archivo tal que el tiempo sea del orden de 0,5 seg sin i/o. Explique los resultados

Cipher	Tiempo de encriptación en segundos	Tiempo de encriptación en ciclos de reloj	Tiempo de descriptación en segundos	Tiempo de descriptación en ciclos de reloj
Triple DES	0.600081	1,916,716,563	0.613080	1,958,234,820
RSA	2.748630	8,779,387,088	68.157385	217,701,175,917

Luego de realizada la encriptación y descriptación con triple DES y RSA, descubrimos que Triple DES tarda menos tanto en la encriptación como en la descriptación que RSA.