
	<p align="center">UNIVERSIDAD NACIONAL DE SAN AGUSTIN FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA</p>	
Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación		
Aprobación: 2022/03/01	Código: GUIA-PRLD-001	Página: 1

GUÍA DE LABORATORIO 02

INFORMACIÓN BÁSICA					
ASIGNATURA:	<i>SEGURIDAD INFORMÁTICA</i>				
TÍTULO DE LA PRÁCTICA:	<i>CRIPTOGRAFÍA CLÁSICA: CIFRADO MONOALFABÉTICO Y POLIALFABÉTICO</i>				
NÚMERO DE PRÁCTICA:	<i>01</i>	AÑO LECTIVO:	<i>2023</i>	NRO. SEMESTRE:	<i>A</i>
TIPO DE PRÁCTICA:	INDIVIDUAL				
	GRUPAL	MÍNIMO DE ESTUDIANTES	<i>1</i>	MÁXIMO DE ESTUDIANTES	<i>2</i>
FECHA INICIO:	<i>16/06/2023</i>	FECHA FIN:	<i>22/06/2023</i>	DURACIÓN:	<i>7 días</i>
RECURSOS Y EQUIPOS A UTILIZAR: <i>PC, IDE de Programación</i>					
DOCENTE(s): <i>Juan Carlos Zuñiga</i>					

OBJETIVOS/TEMAS Y COMPETENCIAS	
OBJETIVOS:	<ul style="list-style-type: none"> <i>Implementar algoritmos de cifrado y descifrado monoalfabético</i> <i>Implementar algoritmos de cifrado y descifrado polialfabético</i>
TEMAS:	<ul style="list-style-type: none"> <i>Cifrado monoalfabético y polialfabético</i> <i>Cifrado de César</i> <i>Cifrado Vignere</i> <i>Cifrado Autoclave</i> <i>Criptografía</i> <i>Ataque Kasiski</i>
COMPETENCIAS A ALCANZAR	<p><i>Mantiene responsablemente, software para que se adecue a las necesidades cambiantes del usuario, cliente o sociedad mediante la aplicación de técnicas y procedimientos establecidos que siguen estándares de calidad destinados a implementar la seguridad informática. (referencia C.n)</i></p> <p><i>Asegura la calidad del software mediante la aplicación de pruebas, validaciones y estándares de seguridad para garantizar el correcto funcionamiento del producto, en el marco de la seguridad informática, considerando el impacto productivo y social. (referencia C.o)</i></p> <p><i>Diseña soluciones informáticas apropiadas para proveer seguridad informática, utilizando los principios de ingeniería que integran consideraciones éticas, sociales, legales y económicas entiendo las fortalezas y limitaciones del contexto (referencia C.q)</i></p>

CONTENIDO DE LA GUÍA

I. MARCO CONCEPTUAL

1. Cifrado Monoalfabético

Estas técnicas de cifrado simplemente sustituyen un carácter del alfabeto de origen por un carácter en el alfabeto de llegada, el más conocido de estos es el cifrado de César, que hace una sustitución a partir de un desplazamiento de tres posiciones según se muestra, en un alfabeto módulo 27.

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

La palabra CASA se cifraría como FDVD.

La cifra del César tiene por tanto una representación matemática para letras mayúsculas en castellano del tipo:

$$C = M + 3 \bmod 27$$

En donde **M** es la posición en el alfabeto de la letra del texto en claro que se cifra y **C** la posición donde recuperamos el carácter a introducir en el criptograma resultante. Por lo tanto, de forma genérica diremos que el cifrador del César con un desplazamiento de 3 espacios, es un caso particular de un cifrado de sustitución por desplazamiento puro de la forma:

$$C = M + b \bmod n$$

Donde **n** es el tamaño del alfabeto del texto claro y el del aly del módulo de cifra y **b** es la constante de desplazamiento. Observa que dicha constante puede tomar valores desde 1 hasta n-1, en tanto un desplazamiento b = 0 o bien b = n enviaría el texto en claro.

La desventaja clara de estas técnicas de cifrado es que el cypher mantiene exactamente la misma distribución frecuencial que el alfabeto del texto claro, lo que facilita el ataque

2. Cifrado Polialfabético

En los cifrados polialfabéticos la sustitución aplicada a cada caracter varía en función de la posición que ocupe este dentro del texto claro. En otro sentido, corresponde a una aplicación cíclica de n cifrados de sustitución monoalfabetica.

2.1 Cifrado de Vignere

En el siglo XVI el criptógrafo francés propone el más conocido de los métodos de cifrado polialfabético, invulnerable por más de 300 años, basada en matemáticas discretas, usa una tabla normalmente con alfabetos de mayúsculas con 26 o 27 caracteres, donde cada fila es la anterior desplazada una posición

a la izquierda, las columnas se usan para el mensaje claro y las filas para la clave repetida cíclicamente tantas veces como se le necesite

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

Por ejemplo, el cifrado de **HERMOSO** a partir de la clave **CIELO** será la respuesta no lineal

H	E	R	M	O	S	O
C	I	E	L	O	C	I
J	M	V	W	D	U	W

Usando matemáticas discretas, se escribe la clave debajo del texto claro tantas veces como se necesite y considerando la ubicación de las letras en el alfabeto

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

Se implementa el algoritmo

$$c_i = m_i + k_i \bmod(n)$$

como se muestra

H	E	R	M	O	S	O
7	4	18	12	15	19	15
C	I	E	L	O	C	I
2	8	4	11	15	2	8
$7+2=9$	$4+8=12$	$18+4=22$	$12+11=23$	$15+15=30$	$19+2=21$	$15+8=23$
mod 27	mod 27	mod 27	mod 27	mod 27	mod 27	mod 27
9	12	22	23	3	21	23
J	M	V	W	D	U	W

El proceso de descifrado aplicando matemáticas discretas sería:

$$m_i = c_i - k_i \bmod(n)$$

$$m_i = c_i - (n - k_i) \bmod(n)$$

Para el cifrado anterior:

J	M	V	W	D	U	W
9	12	22	23	3	21	23
C	I	E	L	O	C	I
2	8	4	11	15	2	8
$9-2=7$	$12-8=4$	$22-4=18$	$23-11=12$	$3-15=-12$	$21-2=19$	$23-8=15$
mod 27	mod 27	mod 27	mod 27	mod 27	mod 27	mod 27
7	4	18	12	15	19	15
H	E	R	M	O	S	O

2.2 Cifrado Autoclave

La debilidad evidente de Vigenère es el hecho de que el cifrado es periódico, por lo que se irá repitiendo a largo del mensaje, lo que facilitará el criptoanálisis. Se puede usar una variante del sistema Vigenère conocida como autoclave y que consiste en:

- Se escribe la clave
- Al llegar a la última letra de esa clave, ésta ya no se repite
- Se continúa la clave con el propio mensaje en claro a continuación

Por ejemplo, el cifrado de **AUTOCLAVE** con la clave **LUNA** sería:

A	U	T	O	C	L	A	V	E
0	21	20	15	2	11	0	22	4
L	U	N	A	A	U	T	O	C
11	21	13	0	0	21	20	15	2
$0+11=11$	$21+21=42$	$20+13=33$	$15+0=15$	$2+0=-2$	$11+21=32$	$0+20=20$	$22+15=37$	$4+2=6$
mod 27	mod 27	mod 27	mod 27	mod 27	mod 27	mod 27	mod 27	mod 27
11	15	6	15	2	5	20	10	6
L	O	G	O	C	F	T	K	G

3. Criptoanálisis: el ataque Kasiski

Kasiski observó la existencia de secuencias de caracteres repetidos en el texto cifrado (poligramas) lo cual significaba casi con toda probabilidad que dichas secuencias no sólo eran la misma antes del cifrado, sino que además la clave debía coincidir en la misma posición, en esto basó su ataque, en detectar secuencias de letras cifradas repetidas.

Por ejemplo, para el siguiente criptograma, se puede implementar la búsqueda de cadenas repetidas:

LNUDVMUYRMUDVLLPXAFZUEFAIOVWVMUOVMUEVMUEZCU
DVSYWCIVCFGUCUNYCGALLGRCTIJTRNNPJQOPJEMZITYLIA
YKRYEFDUDCAMAVRMZEAMBLEXPJCCQIEHPJTYXVNMLAEZTI
MUOFRUFC

Es decir:

- 3 cadenas "UDV" separadas por 8 y 32 posiciones.
- 2 cadenas "MUE" separadas por 4 posiciones.
- 2 cadenas "MUO" separadas por 108 posiciones.

Luego podemos pensar que el número de caracteres de la clave puede ser $L = \text{mcd}(4, 8, 32, 108) = 4$. Es decir, la longitud más probable de la clave es $L=4$, que es el máximo común divisor.

A partir de esta presunción se divide el cripto en L subcriptogramas formados por las letras cada L posiciones

Primer subcriptograma:

LNUDV MUYRM UDVLL PXAFZ UEFAI OVWVM UOVMU EVMUE ZCUDV
SYWCI VCFGU CNYC GALLG RCYTI JTRNN PJQOP JEMZI TYLIA
YKRY EFDUD CAMAV RMZEA MBLEX PJCCQ IEHPJ TYXVN MLAEZ
TIMUO FRUFC

$C_A = \text{LVRVXUIVVZVCFUGGTRJJIIKFCVELJIVJAIFC}$

Segundo subcriptograma:

LNUDV MUYRM UDVLL PXAFZ UEFAI OVWVM UOVMU EVMUE ZCUDV
SYWCI VCFGU CNYC GALLG RCYTI JTRNN PJQOP JEMZI TYLIA
YKRY EFDUD CAMAV RMZEA MBLEX PJCCQ IEHPJ TYXVN MLAEZ
TIMUO FRUFC

$C_B = \text{NMMLAEOMMMCSIGNARINQETARDARAECETNEMR}$

Tercer subcriptograma:

LN \underline{U} DV MU \underline{Y} RM \underline{U} DVLL PXAFZ UEFAI O \underline{V} WVM \underline{U} OVM \underline{U} EVM \underline{U} E ZC \underline{U} DV
SY \underline{W} CI \underline{V} CFG \underline{U} CUN \underline{Y} C GALLG RC \underline{Y} TI \underline{J} TRNN \underline{P} JQOP JEM \underline{Z} I TY \underline{L} IA
YY \underline{K} RY EFD \underline{U} D CAM \underline{A} AV RM \underline{Z} EA MB \underline{L} EX \underline{P} JCCQ IE \underline{H} PJ TY \underline{X} VN \underline{M} LAEZ
TIM \underline{U} O FR \underline{U} FC

$C_c =$ UUULFFVUUUUUYVUYLCJNOMYYYUMMMXCHYMZUU

Tercer subcriptograma:

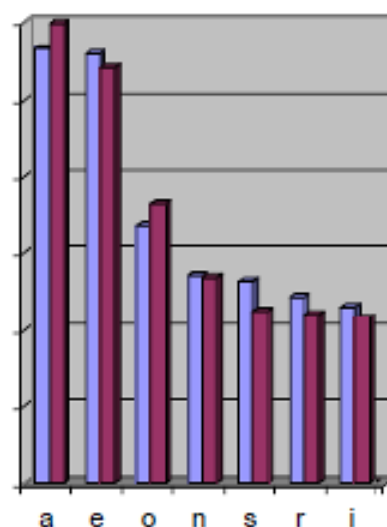
LN \underline{U} DV MU \underline{Y} RM \underline{U} DVLL PXAFZ UEFAI O \underline{V} WVM \underline{U} OVM \underline{U} EVM \underline{U} E ZC \underline{U} DV
SY \underline{W} CI \underline{V} CFG \underline{U} CUN \underline{Y} C GALLG RC \underline{Y} TI \underline{J} TRNN \underline{P} JQOP JEM \underline{Z} I TY \underline{L} IA
YY \underline{K} RY EFD \underline{U} D CAM \underline{A} AV RM \underline{Z} EA MB \underline{L} EX \underline{P} JCCQ IE \underline{H} PJ TY \underline{X} VN \underline{M} LAEZ
TIM \underline{U} O FR \underline{U} FC



$C_c =$ UUULFFVUUUUUYVUYLCJNOMYYYUMMMXCHYMZUU

Luego en cada subcriptograma se implementa un análisis estadístico de frecuencias por caracter:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C _A	1	0	3	0	1	3	2	0	5	4	1	2	0	0	0	0	0	2	0	1	2	8	0	1	0	1	
C _B	5	0	2	1	5	0	1	0	2	0	0	1	6	4	0	1	0	1	4	1	2	0	0	0	0	0	
C _C	0	0	2	0	0	2	0	1	0	1	0	2	5	1	0	1	0	0	0	0	0	11	2	0	1	6	1
C _D	2	1	3	4	3	1	0	0	0	0	0	3	0	0	0	2	5	1	0	0	2	0	0	2	1	3	3

Análisis de Frecuencias (%)



	<p style="text-align: center;">UNIVERSIDAD NACIONAL DE SAN AGUSTIN FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA</p>	
<p style="text-align: center;">Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación</p>		
<p>Aprobación: 2022/03/01</p>	<p>Código: GUIA-PRLD-001</p>	<p>Página: 7</p>

II. EJERCICIO RESUELTO

Revisar sobre el ataque Kasiski: <https://www.youtube.com/watch?v=A7p2ydEPg1k>

Mensaje cifrado:

```

MOMUDEKAPVTQEFMOEVHPAJMIICDCTIFGYAGJSPXYALUYMNSMYH
VUXJELEPXJFXGCMJHKDZRYICUHYPU SPGIGMOIYHFWHTCQKMLRD
ITLXZLJFVQGHOLWCUHLOMDSOECTALUVYLNZRFGBXPHVGALWQIS
FGRPHJOOFWGUBUYILAPLALCAFAAMKLG CETDWVOELJIKGJBXPHVG
ALWQCSNWBUBYHCUHKOC EXJEYKBQKVYKII EHGR LGHXEOLWAWFOJ
ILOVVRHPKDWIHK NATUHNVRYAQDIVHXFHRZVQMMWVLGSHNNLVZS
JLAKIFHXUFXLXMTBLQVRXXHRFZXGVLRAJIEXPVOSMNPKEPDT
LPRWMJAZPKLQUZAALGZXGVLKLGJTUIITDSUREZXJERXZSHMPST
MTEOEPAPJHSMFNBVYVQUZAALGAYDNMPAQOWTUHDBVTSMEUIMVH
QGVRAEFSPEMPVEPKXZYWLKJAGWALT VYVYOBIXOKIHPDSEVLEV
RVSGBJOGYWFHKBGLXYAMVKISKIEHYIMAPXUOISKPVAGNMZHPW
TTZPVXFCCDTUJHJWLAPFYULTBUXJLNSIJVVYOVDJSOLXGTGRVO
SFRIICTMKOJFCQFKTINQBWWHGTENLHHOGCSPSPFVVGJOKMSIFPR
ZPAASATPTZFTFPDPORRFTAXZPKALQAWMIUDBWNCTLEFKOZQDLX
BUXJLASIMRPNMBFZCYLVWAPVVFQRHZVZGZEFKBYIOOFXYEVOWGB
BXVCBXBAGLQKCMICRRXMACUOIKHQUAJEGLOIJHXPVZWJEWBA
FWAMLZZRXJEKAHV FASMULVVUTT GK

```

Determinando para una longitud de clave de 14 caracteres, los subcriptogramas

```

C1
MMTUERMROTPHLTPBKGOTFNUXLAUAAATVPWIBYAZTBDRTHMTXWBFZXBMLBAG
C2
OOIPYODLAHJADHYBHVUHNHFPPAIZPAUHVAHJAPHUUJIIOSZZNUZVYAAOAHK
C3
MEFMXIIIWLVOLWVHQXVHRLXRRRLISJLHQELPOMXPHXSINGIFPCXCZEWCFV
C4
UVGNJCYTCUGOCVGCKERNZVJFWWGTHHGDGPTDGVUWJJOCQCFTKTJYGVGUJWF
C5
DHYSFUHLUVAFQAOUVOHVVLZOMZDMSABVKVSYKOTHLTBSPALLZLOHAA
C6
EPAMXHFXYLWFELHYLPRQSXSJXSPMYVRXYEWIITWNXMWPRPLEAVEWQJHMS
C7
KAGYGYWZLLW GALWKKWKYWMGMAGUSFDTWZYVFSZLSGKVSZDQFSWFGKKXLM
C8
AJJHCPHLONQUAJQOIADAMLT VNZVRTNNSAYOLHKKPAITOHFPKAKIABCHPZU
C9
PMSVMUTJIMZIBMICCIWWQWABLPLEMBMMEWBEKIPVPJGJGPAOWOMPBBMQVZL
C10
VIPUJSCFDRSYKKSEEFIDVKLRKKKZTYPUFLYVBEVXFVRFTVARMZRVYXIUZRV
C11
TIXXHPQVSFFILGNXHOHILIQAE LLXEAESKIRLHAFVVCESRIQPFI VCAWXV
C12
QCYJKGKQGG LGJWJGJKVGFVJPQGJOQQUPJXVGYGCUYOQNJAFUDNQOCRJUU
C13
EDAEDIMGEBRACBBE RINHSRIDUJEEUOIEAOSLINCLOSLOTDLMROBREET
C14
FCLLZGLHKXPPEXUYLLAXHXXETZTRPZWMMGKGXMMMDTVFKHKPABXBHFXXGWKT

```


Si se sabe que el idioma es el inglés, consideramos las distribuciones frecuenciales del mismo

e	12,702%
t	9,056%
a	8,167%
o	7,507%
i	6,966%
n	6,749%
s	6,327%
h	6,094%
r	5,987%
d	4,253%
l	4,025%
c	2,782%
u	2,758%
m	2,406%
w	2,361%
f	2,228%
g	2,015%
y	1,974%
p	1,929%
b	1,492%
v	0,978%
k	0,772%
j	0,153%
x	0,150%
q	0,095%
z	0,074%

Hallamos la frecuencia de estos caracteres en cada subcriptograma

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1	5	6	0	1	1	2	2	2	1	0	1	3	5	1	2	3	0	3	0	8	3	1	2	5	1	2
C2	9	1	0	2	0	1	0	9	4	3	1	1	0	2	5	5	0	0	1	0	5	3	0	0	4	4
C3	0	0	3	0	3	3	1	4	7	1	0	6	3	1	2	3	2	4	2	0	0	4	3	6	0	1
C4	0	0	6	2	1	3	9	2	0	6	2	0	0	2	2	1	1	1	0	5	4	6	3	0	2	1
C5	7	2	0	2	0	2	0	5	0	0	2	8	2	0	6	2	0	0	4	2	3	6	0	0	2	4
C6	2	0	0	0	5	2	0	4	3	1	0	4	4	1	0	5	2	3	4	1	0	2	5	7	4	0
C7	3	0	0	2	0	4	7	0	0	1	7	5	3	0	0	0	1	0	6	1	1	2	7	1	4	4
C8	8	1	2	1	0	1	0	5	3	3	4	3	1	4	4	5	2	1	1	3	2	2	0	0	1	2
C9	2	6	2	0	3	0	2	0	4	3	1	3	9	0	2	7	2	0	1	1	1	3	5	0	0	2
C10	1	1	1	2	3	5	0	0	3	1	6	2	1	0	0	2	0	6	3	2	3	8	0	2	4	3
C11	4	0	2	0	4	4	2	4	7	0	1	5	0	1	1	2	3	2	3	1	0	6	1	5	1	0
C12	1	0	3	1	0	2	9	0	0	11	3	1	0	2	4	2	7	1	0	0	4	3	1	1	3	0
C13	3	4	2	4	10	1	1	2	5	1	0	4	2	2	5	0	0	5	3	3	2	0	0	0	0	0
C14	2	2	1	1	2	3	4	4	0	0	5	5	4	0	0	4	0	1	0	4	1	1	2	9	1	3

Buscando en cada subcriptograma las 4 letras que cumplan con la distribución más frecuente de las letras en inglés, "E", "T", "A" y "O".

Para ello, considerando que la posición relativa de la letra "A" es el valor 0, la letra "E" está 4 espacios a la derecha de la "A", la letra "O" está 10 de la "E" y la letra "T" a 5 de la "O", buscaremos en cada subcriptograma los caracteres más frecuentes que cumplan con esa distribución: 0, +4, +10, +5 mod 26.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
C1	16	14	3	8	7	11	8	11	14	6	5	9	12	12	4	13	4	7	7	20	6	5	11	14	9	4	T
C2	14	12	3	11	5	8	10	22	5	5	12	10	10	3	15	11	8	5	2	9	15	15	15	2	4	9	H
C3	5	6	10	11	18	4	2	14	13	11	2	13	8	6	11	10	6	11	12	13	8	8	6	14	10	4	E
C4	8	8	22	8	1	16	16	8	3	14	8	3	4	12	10	8	12	12	12	7	8	15	6	1	9	5	C
C5	15	9	6	7	4	6	9	26	4	0	12	14	11	2	15	6	3	10	12	9	5	16	11	10	4	10	H
C6	8	7	4	12	19	8	0	12	12	9	4	14	10	4	8	9	8	7	13	16	8	3	12	13	11	5	E
C7	4	5	10	9	7	10	19	10	10	2	13	9	11	7	6	3	3	13	25	5	5	7	17	7	7	12	S
C8	15	9	6	7	4	8	8	18	5	9	10	10	12	6	12	12	7	8	4	9	10	11	17	6	5	8	H
C9	8	14	9	5	8	4	6	8	24	5	3	15	13	8	5	12	9	4	11	10	5	10	15	11	11	3	I
C10	6	11	9	8	11	12	12	11	5	4	12	10	7	7	4	9	7	25	5	5	10	12	9	5	12	8	R
C11	10	6	13	7	19	6	3	19	8	8	3	11	11	5	10	10	7	13	11	10	9	7	8	13	5	4	E H
C12	5	8	22	3	1	16	16	5	1	17	11	3	10	12	7	3	22	9	11	1	9	18	7	9	7	3	C Q
C13	21	7	3	11	18	5	3	9	11	5	9	14	6	12	12	12	13	6	8	7	9	6	3	8	9	9	A
C14	8	10	6	8	11	8	13	12	8	10	7	14	9	7	5	9	3	10	11	21	2	4	13	16	7	4	T

Para el primer subcriptograma los caracteres más frecuentes que cumplen con esa distribución son (T, X, H, M), para el segundo (H, L, V, A) y así sucesivamente. Con ello tendríamos la clave. Aunque para los subcriptogramas 11 y 12 hay dos letras que cumplen con esa distribución, vistos el resto de los caracteres de la clave, buscamos una opción con sentido. ésta es: THECHESHIRECAT (el gato de Cheshire creado por Lewis Carroll).

Con esa clave y utilizando la tabla del método de Vigenère, el mensaje en claro sería:

THISWASTHEPOEMTHATALICEREADJABBERWOCKYTWASBRIL
LIGANDTHESLITHYTOVESDIDGYREANDGIMBLEINTHEWABEAL
LMIMSYWERETHEBOROGVESANDTHEMOMERATHSOUTGRAB
EBEWARETHEJABBERWOCKMYSONTHEJAWSTHATBITETHECLA
WSTHATCATCHBEWARETHEJUBJUBBIRDANDSHUNTHEFRUMIO
USBANDERSNATCHHETOOKHISVORPALSWORDINHANDLONGTI
METHEMANXOMEFOEHESOUGHTSORESTEDHEBYTHETUMTUM
TREEANDSTOODAWHILEINTHOUGHTANDASINUFFISHTHOUGHT
HESTOODTHEJABBERWOCKWITHEYESOFFLAMECAMEWHIFFLI
NGTHROUGHTHETULGEYWOODANDBURBLEDASITCAMEONET
WOONETWOANDTHROUGHANDTHROUGHTHEVORPALBLADEW
ENTSNICKERSNACKHELEFTITDEADANDWITHITSHEADHEWENT
GALUMPHINGBACKANDHASTTHOUSLAINTHEJABBERWOCKCO
METOMYARMSMYBEAMISHBOYOFFRABJOUSDAYCALLOOHCAL
LAYHECHORTLEDINHISJOYTWASBRILLIGANDTHESLITHYTOVE
SDIDGYREANDGIMBLEINTHEWABEALLMIMSYWERETHEBOROG
OVESANDTHEMOMERATHSOUTGRABEITSEEMSVERYPRETTYSH
ESAIDWHENSHEHADFINISHEDITBUTITSRATHERHARDTOUNDER
STAND

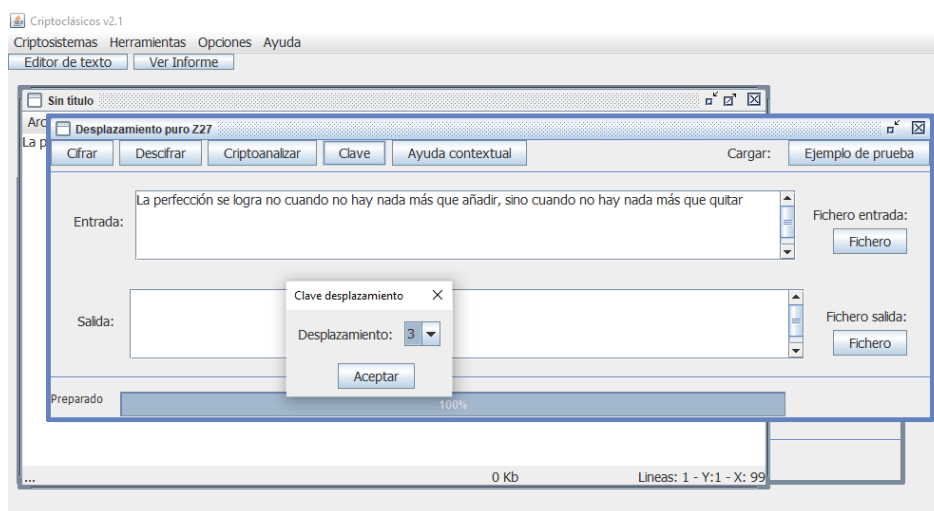
Introduciendo los espacios en blanco para separar las palabras tenemos:

THIS WAS THE POEM THAT ALICE... SEEMS VERY PRETTY SHE
SAID WHEN SHE HAD FINISHED IT BUT ITS RATHER HARD TO
UNDERSTAND.

III. EJERCICIOS PROPUESTOS



Cifrado de César

1. Implementar un algoritmo para construir un cifrador desplazamiento, basado en el cifrado de César, donde el desplazamiento sea elegible, trabajando sobre un alfabeto módulo 27. Se debe ingresar el texto claro (en archivo o por interface) y genere la cifra resultante
2. Verificar cifrando *“La perfección se logra no cuando no hay nada más que añadir, sino cuando no hay nada más que quitar”* Usando un **desplazamiento puro** de 3
3. Verificar el resultado obtenido a partir del cifrador **Criptoclásicos v2.1** (https://www.criptored.es/software/sw_m001c.htm) haciendo las capturas de pantalla respectivas para los datos indicados e incorporando el proceso de cifrado



4. Identifique en el cypher cuál es el carácter que aparece mayor cantidad de veces y demuestre que este representa a la letra “e”, use la herramienta seleccionando **Criptoanalizar**



	<p style="text-align: center;">UNIVERSIDAD NACIONAL DE SAN AGUSTIN FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA</p>	
<p style="text-align: center;">Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación</p>		
<p>Aprobación: 2022/03/01</p>	<p>Código: GUIA-PRLD-001</p>	<p>Página: 11</p>

5. Proponga un algoritmo de descifrado y demuestre su funcionamiento correcto comparando con el resultado mostrado en la herramienta

Cifrado de Vignere

6. Implementar un algoritmo para construir un cifrador de Vignere, donde se pueda seleccionar el módulo, alfabeto módulo 27 o módulo 191 (ASCII), ingresar el texto claro (en archivo o por interface) y genere la cifra resultante
7. Verificar cifrando *“La perfección se logra no cuando no hay nada más que añadir, sino cuando no hay nada más que quitar”* Usando la clave *MEZCLADOR*
8. Verificar el resultado obtenido a partir del cifrador Criptoclásicos v2.1 (https://www.cryptored.es/software/sw_m001c.htm) haciendo las capturas de pantalla respectivas para los módulos 27 y 191
9. Muestre las frecuencias de cada letra del mensaje original usando como claves MALEFICIO, QUESO y MIA, compare y comente sobre la variación de las frecuencias en base a la longitud de la clave
10. Desarrolle un algoritmo que encuentre el texto claro si recibió la cifra

GYLKWQRVEBTPXDJRQDDVQNP HHGQGUGWRNPPWHRGCONLJOHMÑCOXEEAVASIÑDOEQP
ETAPVHEOPEKRXYA EVRUHAÑVNRSIVPZBSXINLEWSMGBSHEEITVDEENSVR



y se sabe que ha cifrado con la clave PEDRONAVAJA

11. Usando el software anterior, verifique el resultado, eligiendo el cifrado Vignere con módulo 27, muestre el informe y comente
12. Usando matemáticas discretas, descifre manualmente YGVMSSKKOX si la clave fue FORTALEZA en un alfabeto de 27 caracteres

Cifrado con autoclave

13. Descifre el texto, usando la clave UNODELOSMASGRANDESCRIPTOGRAFOS:

XHGDQESDMPKÑDEEDKNGJZPFJSUIFZOLFCINFJCESVZTGBFXCIUDAYNUUDIZYWWZBEYNVQWIV
UNKZEPHDODQUZZLBDNDRWTHQSERÑIVMLERCMGIFLSORZXTSDIGLOXQSDJHWVCIWQXQJCK
MBPOKMPSKMUVIMNJDNLCSZHXHNYYUIXDBSOXHZLXWVGDJGXHWLTDWKÑSAQIMZLNBMV
LXHUOQQXIQGWGUFTWKZKMOKUDNINSIFJDUOZIJBVSVOVFAIEÑGYOWPSOAP

	<p align="center">UNIVERSIDAD NACIONAL DE SAN AGUSTIN FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA</p>	
Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación		
Aprobación: 2022/03/01	Código: GUIA-PRLD-001	Página: 12

Ataque de Kasiski

14. Criptoanalizar el siguiente criptograma mod 27, encontrar la clave y el texto en claro.

MAXYHGAVAPUUGZHEGZQOWOBNIPQKRÑMEXIGONIICUCAWIGCTEAGMNOLRSZJNLWÑAW
WIGLDDZSNIZDNBIXGZLAYMXÑCVEKIETMOEOPBEWPTNIXCXUIHMECXLNOCECYEQPBWUFANI
ICÑJIKISCZUAILBGSOANKBFWUAYWNSCHLCWYDZHDZAQVMPTVGFGPVAJWFVPUOYMXCWERV
LQCZWEICFVITUZSNCZUAIBFMÑALIEGLBSZLQUXÑOHWOCGHNYWÑQKDANZUDIFOIMXNPHN
UWQOKLMVBNNKRMKONDPDPNMIKAWOXMEEIVEKGBGSFHVADWPGOYMHIOUEEIPGOLENZB
SCHAGKQTZDRÑMÑNWTUZIÑCMÑAXKQUWDLVANNIHLÑCQNWGEHIPGZDTZTÑNWÑEEWFUM
GIÑXNTWXNVIXCZOAZSOQUVENDNFWUSZYHGLRACPGGUGIYWHOTRMZUGQQDDZIFWHVVS
HCUGOGIFKBXAPBOBRDVDUCMVTGKIGKDRSZLUQSDVPMXVIVEYMFGEANIMQLHLGPQOHRYW
CFEWOISNÑPUAYINNÑXNÑPGKWGOILQGAFOILQTAHEIIDWMÑEÑXNEPRCVDQTURSK

IV. CUESTIONARIO

1. En el ataque a Vigenere por Kasiski ¿Qué buscamos preferentemente?
2. Encontradas las cadenas repetidas en el criptograma, con separación d1, d2, d3 y d4 ¿Cuál sería la longitud L de la clave?
3. Si las distancias entre repeticiones de cadenas en un criptograma son 35, 112, 70. ¿Cuál sería la longitud L de la clave?
4. ¿Qué diferencia la regla AEOS de AEO en Kasiski?

V. REFERENCIAS Y BIBLIOGRAFÍA RECOMENDADAS:

García Arnau, M. (2003). Criptografía clásica. ¿Cómo romper cifrados monoalfabéticos y polialfabéticos? Análisis de frecuencias y método Kasiski. *Buran*, (19), 95-97.

TÉCNICAS E INSTRUMENTOS DE EVALUACIÓN	
TÉCNICAS: <i>Ejercicios propuestos</i>	INSTRUMENTOS: <i>Lista de cotejo</i>
CRITERIOS DE EVALUACIÓN Y LOGROS ALCANZADOS	
<i>Niveles de logro: inicio, proceso, logro esperado, logro destacado.</i>	