

UNIVERSIDAD DEL VALLE DE GUATEMALA

Cifrado de Información

Sección 10

Ludwing Cano



Excelencia que trasciende

DELVALLE
GRUPO EDUCATIVO

Laboratorio 1 A

Encriptado y Decriptado de Texto

José Daniel Gómez Cabrera 21429

Repositorio

<https://github.com/JDgomez2002/cipher/tree/main/lab1/lab1-a>

1. Implementar las funciones de encriptado y decriptado para un texto plano en castellano (27 letras) para los siguientes métodos (30 puntos) a. Cifrado Caesar b. Cifrado afín c. Cifrado Vigenère Para cada método, muestre ejemplos sencillos de encriptado y decriptado (para verificar que funcionan correctamente).

Sugerencia:

- Para implementar funciones para encriptar y decriptar probablemente antes se deba construir una función que limpie el texto plano, removiendo caracteres no alfabéticos

César - Original: HOLA MUNDO

César - Cifrado: KRÑDOXPGR

César - Descifrado: HOLAMUNDO

Afín - Original: ATACAR AL AMACECER

Afín - Cifrado: IAIRIQIJIÑIRBRBQ

Afín - Descifrado: ATACARALAMACECER

Vigenère - Original: MENSAJE SECRETO

Vigenère - Cifrado: ÑONÑELOSZGTOTK

Vigenère - Descifrado: MENSAJESECRETO

2. Implementar el uso de funciones para generar un análisis de frecuencia de un texto plano. (30 puntos) Sugerencias:

- Para construir una función que calcule la distribución de los caracteres que aparecen en el texto cifrado, se espera que su función calcule las probabilidades (las frecuencias dividido el total de caracteres). (Es recomendable completar las letras que no aparezcan en su texto, con probabilidad 0.)

Análisis de frecuencia del texto original

Texto original para análisis:

Análisis de Frecuencia:

Distribución de frecuencias:

Histograma de frecuencias:

E	=====	17.86%
A	=====	14.29%
I	=====	7.14%
L	=====	7.14%
R	=====	7.14%
D	=====	5.36%
N	=====	5.36%
T	=====	5.36%
U	=====	5.36%
C	=====	3.57%
M	=====	3.57%
O	=====	3.57%
S	=====	3.57%
B	=====	1.79%
G	=====	1.79%
H	=====	1.79%
J	=====	1.79%
Q	=====	1.79%
V	=====	1.79%
F		0.00%
K		0.00%
P		0.00%
Ñ		0.00%
W		0.00%
X		0.00%
Y		0.00%
Z		0.00%

Análisis de frecuencia del texto cifrado

Análisis del texto cifrado:		
Texto cifrado: HÑTXLMRWGHÑDODPFKDHVXPDREUDÑLWHUDULDGHOLJXHÑGHFHUYDPWHV		
Análisis de Frecuencia:		
Total de caracteres: 56		
Distribución de frecuencias:		
Letra	Frecuencia	Porcentaje

H	10	17.8571%
D	8	14.2857%
L	4	7.1429%
Ñ	4	7.1429%
U	4	7.1429%
G	3	5.3571%
P	3	5.3571%
W	3	5.3571%
X	3	5.3571%
F	2	3.5714%
O	2	3.5714%
R	2	3.5714%
V	2	3.5714%
E	1	1.7857%
J	1	1.7857%
K	1	1.7857%
M	1	1.7857%
T	1	1.7857%
Y	1	1.7857%
A	0	0.0000%
B	0	0.0000%
C	0	0.0000%
I	0	0.0000%
N	0	0.0000%
Q	0	0.0000%
S	0	0.0000%
Z	0	0.0000%

```

Histograma de frecuencias:
H |=====| 17.86%
D |=====| 14.29%
L |=====| 7.14%
Ñ |=====| 7.14%
U |=====| 7.14%
G |=====| 5.36%
P |=====| 5.36%
W |=====| 5.36%
X |=====| 5.36%
F |=====| 3.57%
O |=====| 3.57%
R |=====| 3.57%
V |=====| 3.57%
E |=====| 1.79%
J |=====| 1.79%
K |=====| 1.79%
M |=====| 1.79%
T |=====| 1.79%
Y |=====| 1.79%
A | | 0.00%
B | | 0.00%
C | | 0.00%
I | | 0.00%
N | | 0.00%
Q | | 0.00%
S | | 0.00%
Z | | 0.00%

```

```

Process finished with exit code 0

```

3. Implementar una función para comparar la distribución encontrada contra la distribución teórica de las letras del castellano (40 puntos)

Análisis de Frecuencia:

Total de caracteres: 56

Distribución de frecuencias:

Letra	Frecuencia	Porcentaje
-------	------------	------------

E	10	17.8571%
A	8	14.2857%
I	4	7.1429%
L	4	7.1429%
R	4	7.1429%
D	3	5.3571%
N	3	5.3571%
T	3	5.3571%
U	3	5.3571%
C	2	3.5714%
M	2	3.5714%
O	2	3.5714%
S	2	3.5714%
B	1	1.7857%
G	1	1.7857%
H	1	1.7857%
J	1	1.7857%
Q	1	1.7857%
V	1	1.7857%
F	0	0.0000%
K	0	0.0000%
P	0	0.0000%
Ñ	0	0.0000%
W	0	0.0000%
X	0	0.0000%
Y	0	0.0000%
Z	0	0.0000%

Comparación de Distribuciones de Frecuencia:

=====

Letra	Observada	Teórica	Diferencia
-------	-----------	---------	------------

O	3.57	8.68	5.11
S	3.57	7.98	4.41
E	17.86	13.68	4.18
P	0.00	2.51	2.51
L	7.14	4.97	2.17
A	14.29	12.53	1.76
U	5.36	3.93	1.43
N	5.36	6.71	1.35
J	1.79	0.44	1.35
C	3.57	4.68	1.11
H	1.79	0.70	1.09
Q	1.79	0.88	0.91
Y	0.00	0.90	0.90
I	7.14	6.25	0.89
V	1.79	0.90	0.89
G	1.79	1.01	0.78
T	5.36	4.63	0.73
F	0.00	0.69	0.69
Z	0.00	0.52	0.52
D	5.36	5.86	0.50
M	3.57	3.15	0.42
B	1.79	1.42	0.37
Ñ	0.00	0.31	0.31
R	7.14	6.87	0.27
X	0.00	0.22	0.22
K	0.00	0.02	0.02
W	0.00	0.01	0.01

Estadísticas de la comparación:

Diferencia total: 34.87%

Diferencia máxima: 5.11%

Diferencia promedio: 1.29%

Gráfico de Comparación:

(O: Observada, T: Teórica)

	0%	5%	10%	15%
	----- ----- -----			
AT..O.			
B	..TO.....			
CO.T.....			
DOT.....			
EO			
F	OT.....			
G	..TO.....			
H	.T.O.....			
IT.O.....			
J	T..O.....			
K	T.....			
LT...O.....			
MTO.....			
NO..T.....			
OO.....T.....			
P	O....T.....			
Q	.T.O.....			
RTO.....			
SO.....T.....			
TTO.....			
UT..O.....			
V	.T.O.....			
W	T.....			
X	T.....			
Y	OT.....			
Z	OT.....			
Ñ	T.....			

=== Análisis del texto cifrado ===

Análisis de Frecuencia:

Total de caracteres: 56

Distribución de frecuencias:

Letra	Frecuencia	Porcentaje

H	10	17.8571%
D	8	14.2857%
L	4	7.1429%
Ñ	4	7.1429%
U	4	7.1429%
G	3	5.3571%
P	3	5.3571%
W	3	5.3571%
X	3	5.3571%
F	2	3.5714%
O	2	3.5714%
R	2	3.5714%
V	2	3.5714%
E	1	1.7857%
J	1	1.7857%
K	1	1.7857%
M	1	1.7857%
T	1	1.7857%
Y	1	1.7857%
A	0	0.0000%
B	0	0.0000%
C	0	0.0000%
I	0	0.0000%
N	0	0.0000%
Q	0	0.0000%
S	0	0.0000%
Z	0	0.0000%

Comparación de Distribuciones de Frecuencia:

=====

Letra	Observada	Teórica	Diferencia
-------	-----------	---------	------------

H	17.86	0.70	17.16
A	0.00	12.53	12.53
E	1.79	13.68	11.89
D	14.29	5.86	8.43
S	0.00	7.98	7.98
Ñ	7.14	0.31	6.83
N	0.00	6.71	6.71
I	0.00	6.25	6.25
W	5.36	0.01	5.35
X	5.36	0.22	5.14
O	3.57	8.68	5.11
C	0.00	4.68	4.68
G	5.36	1.01	4.35
R	3.57	6.87	3.30
U	7.14	3.93	3.21
F	3.57	0.69	2.88
P	5.36	2.51	2.85
T	1.79	4.63	2.84
V	3.57	0.90	2.67
L	7.14	4.97	2.17
K	1.79	0.02	1.77
B	0.00	1.42	1.42
M	1.79	3.15	1.36
J	1.79	0.44	1.35
Y	1.79	0.90	0.89
Q	0.00	0.88	0.88
Z	0.00	0.52	0.52

Estadísticas de la comparación:

Diferencia total: 130.51%

Diferencia máxima: 17.16%

Diferencia promedio: 4.83%

```

Gráfico de Comparación:
(O: Observada, T: Teórica)
0%      5%      10%     15%
|-----|-----|-----|
A O.....T....
B O.T.....
C O.....T.....
D .....T.....O.
E ...O.....T..
F .T....O.....
G ..T.....O.....
H .....O
I O.....T.....
J T..O.....
K T..O.....
L .....T....O.....
M ...O..T.....
N O.....T.....
O .....O.....T.....
P ....T....O.....
Q OT.....
R .....O....T.....
S O.....T.....
T ...O....T.....
U .....T.....O.....
V .T....O.....
W T.....O.....
X T.....O.....
Y .T.O.....
Z OT.....
Ñ T.....O.....

Process finished with exit code 0

```

La herramienta de inteligencia artificial que utilice como apoyo fue Claude, con el modelo Sonnet 3.5. Este no permite compartir el Chat, por lo tanto, no pude adjuntarlo, pero lo tomé como base para los métodos e infraestructura de las clases para poder facilitar el uso de estas, así como también únicamente el formato impresión del análisis de frecuencia.