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

INFORME DE LABORATORIO

(formato estudiante)

INFORMACIÓN BÁSICA					
ASIGNATURA:	Seguridad Informatica				
TÍTULO DE LA PRÁCTICA:	CRIPTOANALISIS				
NÚMERO DE PRÁCTICA:	03	AÑO LECTIVO:	2023	NRO. SEMESTRE:	A
FECHA DE PRESENTACIÓN	16/06/2023	HORA DE PRESENTACIÓN			
INTEGRANTE (s): Yoset Cozco Mauri				NOTA:	
DOCENTE(s): Juan carlos Zuñiga					

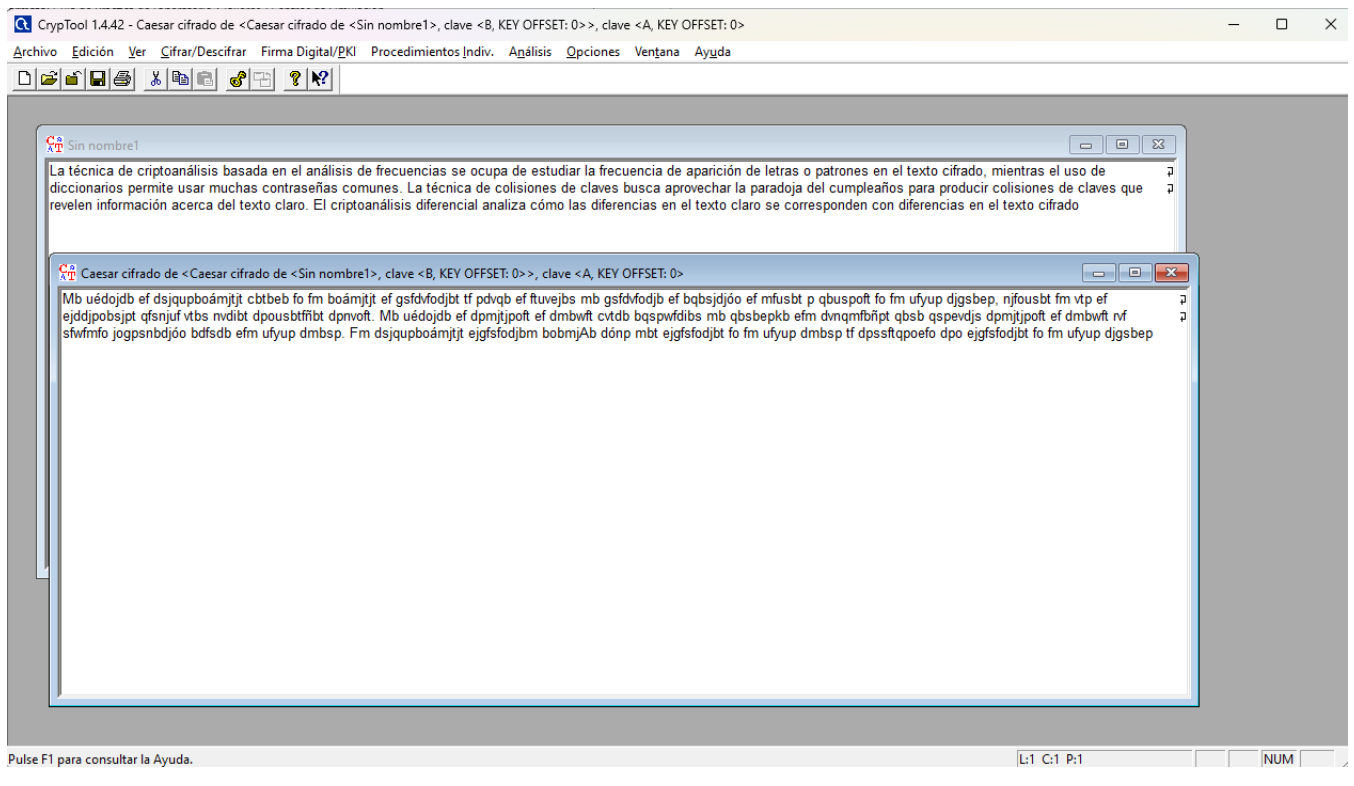
SOLUCIÓN Y RESULTADOS

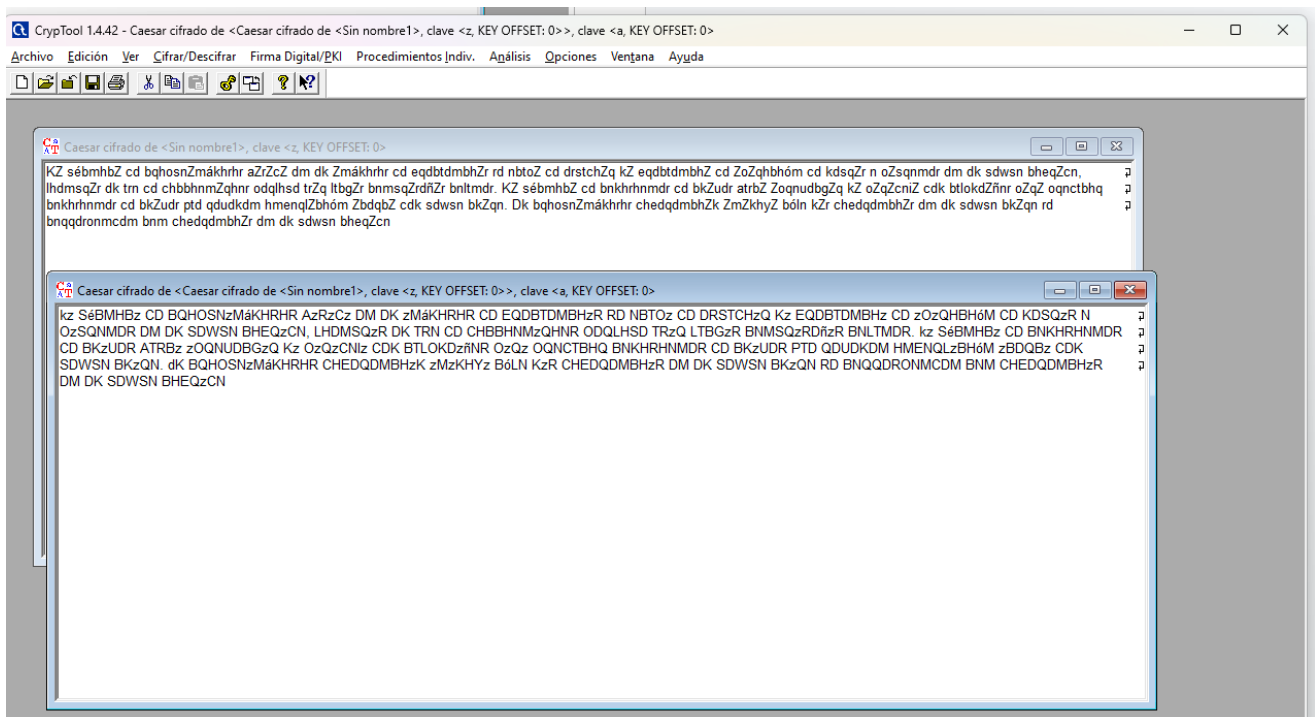
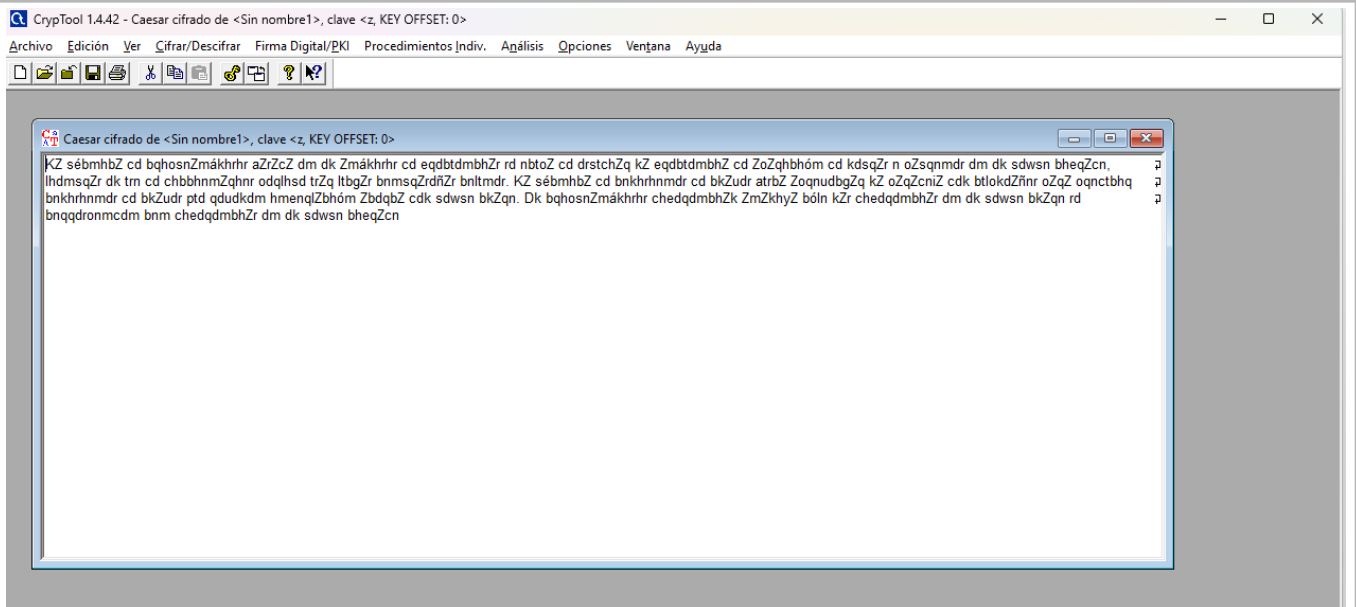
SOLUCIÓN DE EJERCICIOS/PROBLEMAS

1. Para el siguiente texto claro

La técnica de criptoanálisis basada en el análisis de frecuencias se ocupa de estudiar la frecuencia de aparición de letras o patrones en el texto cifrado, mientras el uso de diccionarios permite usar muchas contraseñas comunes. La técnica de colisiones de claves busca aprovechar la paradoja del cumpleaños para producir colisiones de claves que revelen información acerca del texto claro. El criptoanálisis diferencial analiza cómo las diferencias en el texto claro se corresponden con diferencias en el texto cifrado

a) Cifre eligiendo un alfabeto que contenga mayúsculas y minúsculas, utilice las siguientes claves “a”, “A”, “z”





	<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-PRLE-001</p>	<p>Página: 4</p>

Explique los resultado obtenidos:

Podemos afirmar que utilizar la clave "a" no produce ninguna modificación en el texto, mientras que las claves "A" y "Z" generan un desplazamiento de 1 carácter en sentido ascendente y descendente respectivamente, para las letras minúsculas. Las letras mayúsculas permanecen sin cambios en ambos casos.

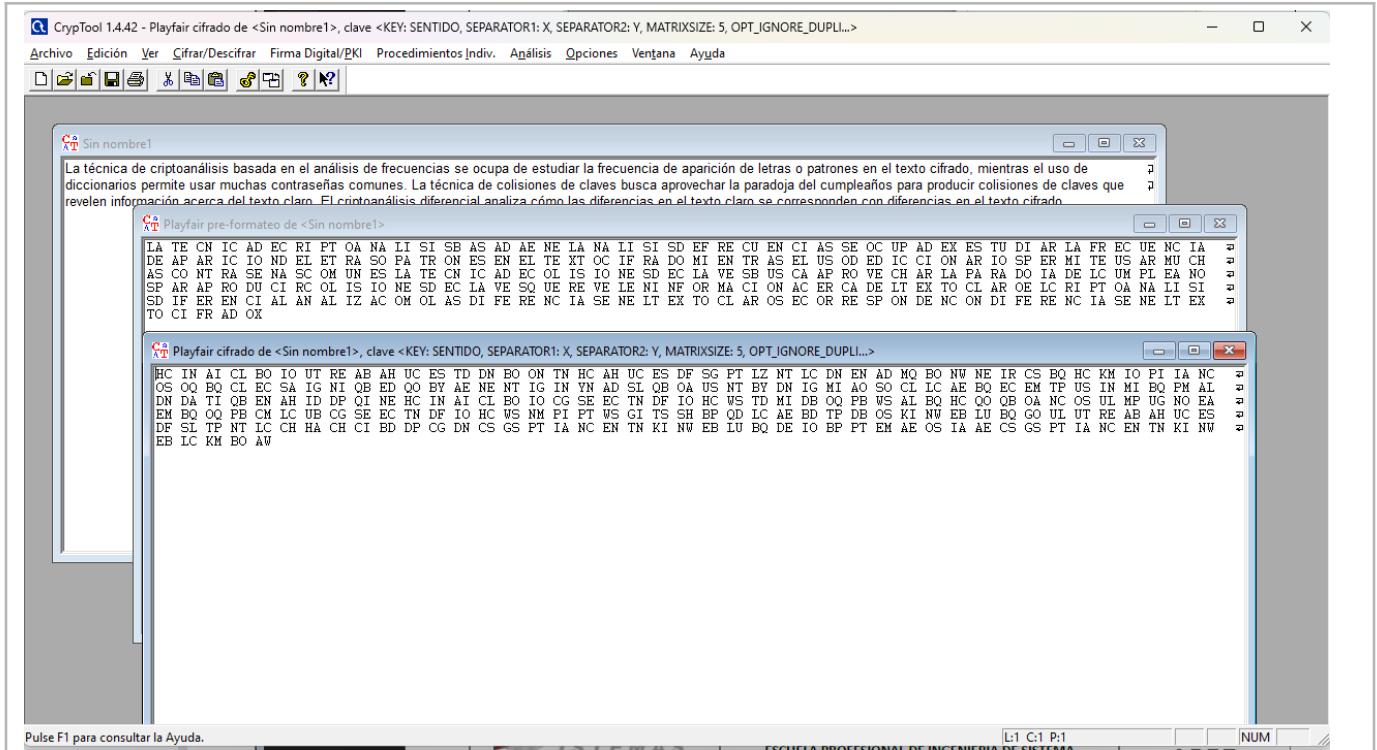
¿Qué otros caracteres se puede añadir al alfabeto?

Se pueden agregar espacios, números, puntuación y diéresis.

2. Playfair: sea el texto claro

La historia de la criptografía es larga y abunda en anécdotas. Ya las primeras civilizaciones desarrollaron técnicas para enviar mensajes durante las campañas militares, de forma que si el mensajero era interceptado la información que portaba no corriera el peligro de caer en manos del enemigo. El primer método de criptografía fue en el siglo V a.C, era conocido como "Escítala". El segundo criptosistema que se conoce fue documentado por el historiador griego Polibio: un sistema de sustitución basado en la posición de las letras en una tabla. También los romanos utilizaron sistemas de sustitución, siendo el método actualmente conocido como César, porque supuestamente Julio César lo empleó en sus campañas, uno de los más conocidos en la literatura (según algunos autores, en realidad Julio César no usaba este sistema de sustitución, pero la atribución tiene tanto arraigo que el nombre de este método de sustitución ha quedado para los anales de la historia). Otro de los métodos criptográficos utilizados por los griegos fue la escítala espartana, un método de trasposición basado en un cilindro que servía como clave en el que se enrollaba el mensaje para poder cifrar y descifrar.

a) Cifre usando una matriz 5x5 con la clave SENTIDO, explique la matriz clave



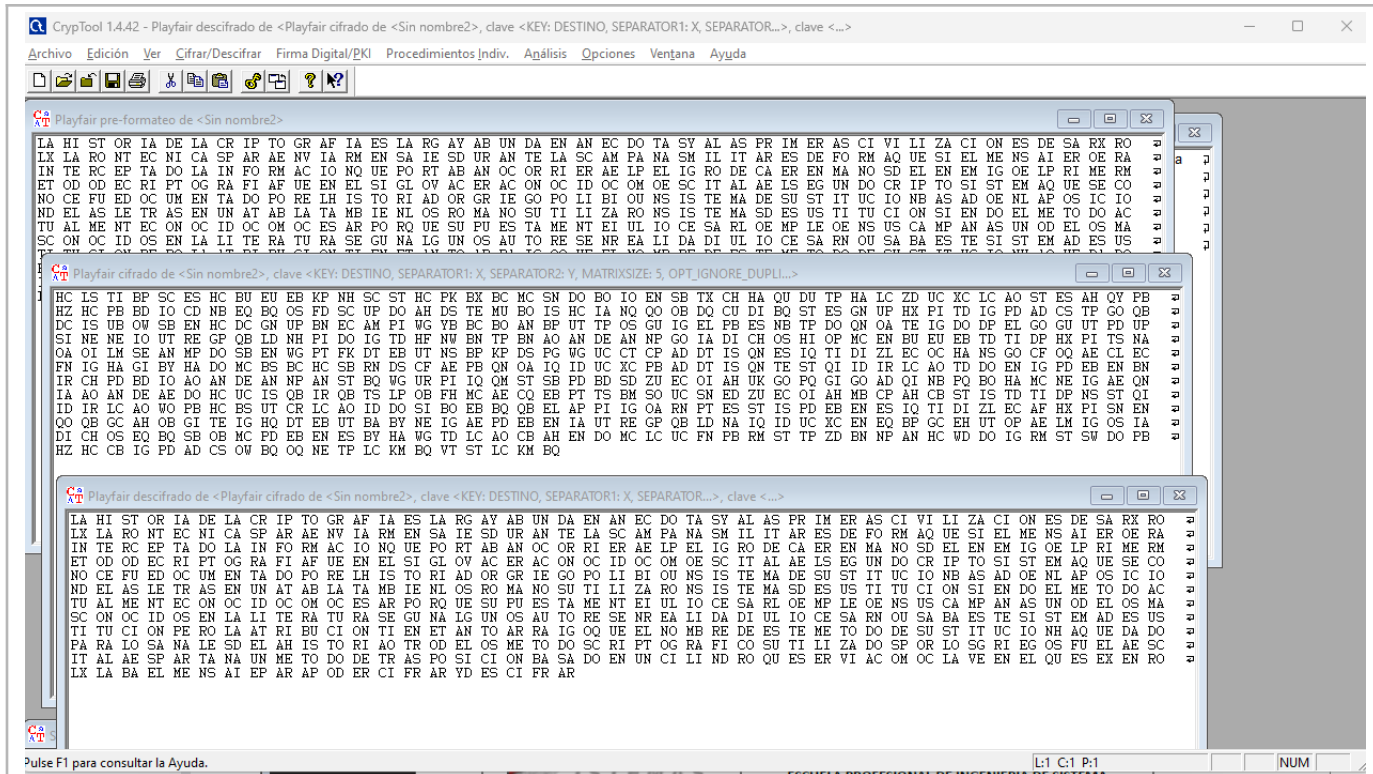
The screenshot shows the CrypTool 1.4.42 interface. The main window displays the 'Playfair pre-formateo de <Sin nombre1>' step, which involves removing punctuation and converting the text to uppercase. The 'Playfair cifrado de <Sin nombre1>' window shows the resulting ciphertext:
 HC IN AI CL BO IO UT RE AB AH UC ES TD DN BO TN HC AH UC ES DF SG PT LZ NT LC DN EN AD MQ BO NW NE IR CS BO HC KM IO PI IA NC
 OS OQ BQ CL EC SA IG NI QB ED QO BY AE NE NT IG IN YN AD SL QB OA US NT BY DN IG MI AO SO CL LC AE BQ EC EM TP US IN MI BQ PM AL
 DN DA TI QB EN AH ID DP QI NE HC IN AI CL BO IO CG SE EC TN DF IO HC VS TD MI DB OQ PB WS AL BQ HC QO QB OA NC OS UL MP UG NO EA
 EM BQ OQ PB CM LC UB CG SE EC TN DF IO HC VS NM PI PT VS GI TS SH BP QD LC AE BD TP DB OS KI NW EB LU BQ GO UL UT RE AB AH UC ES
 DF SL TP NT LC CH HA CH CI BD DP CG DN CS GS PT IA NC EN TN KI NW EB LU BQ DE IO BF PT EM AE OS IA AE CS GS PT IA NC EN TN KI NW
 EB LC KM BO AV

Below the screenshot, the instructions for the task are provided:

b) Explique el resultado mostrado en el pre-procesamiento

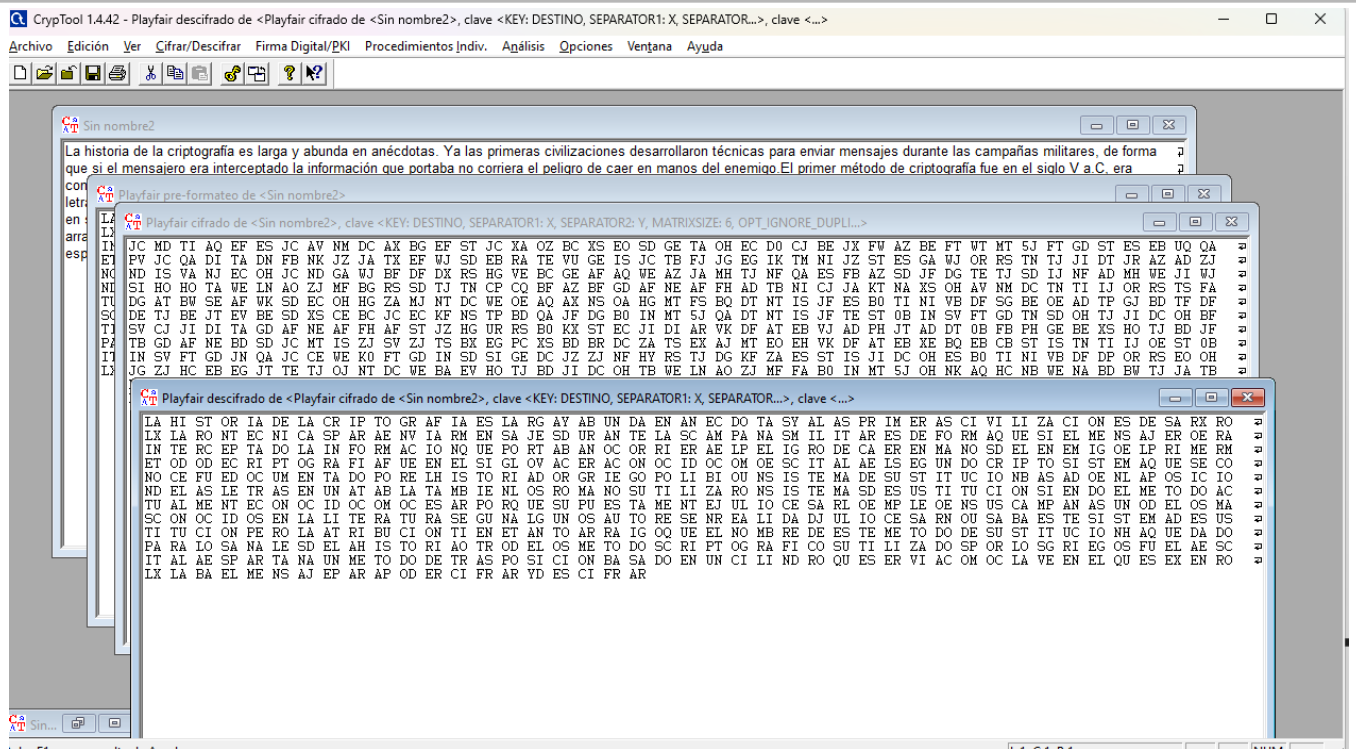
Se han quitado signos de puntuacion, adicional a eso se ha convertido toda la cadena en mayusculas

c) Descifre el resultado, explique lo que se obtiene



Se obtiene el mismo texto cifrado, pero separados en pares de dos letras y en mayúsculas.

d) Cifre con la misma clave usando una matriz 6x6, explique el resultado obtenido, ¿en cuál de los casos aparecieron nuevos caracteres?



En el 6x6 aparecieron nuevos caracteres.

3. El siguiente cipher ha sido capturado, lo único que se sabe es que el idioma original es el inglés

c2cihgQ2O5aM 05hhgMZl YjO 6SkM 5SQtb0mV4 7h 162TUg YfN T0i96WP1m 0g12S5hd8. uV76j MZ5k243YSlg a2 N5n0aKW Thf IRP 6rglOX6 ngaXR 7a2a1 3SkjaMP6, 3b5 3SSk27Y2S jia3P O ecl YQ S83g14 6acmVO P7 ikOO 7h YfKWcs2 IRPWk 0g12S5hfO36. y6fS4S-lh23P OgYd83Wl a63S26g 9K6S 426X 3850623Tn9d8 5671 IY 6Sk678 SOK1oK2S 62kSR1l YfN N2famXTQ3haYY 3kclYN2eg. zY7So2j M2cihgQ2O5aM 05hhgMZl 525P 6ha6 4YWji6 MSOKY43P5bglSN6 p5aMS 0386 3SSbf 2XLZrga2 X2k2 5SQtb0mV4 7aYf 3SOm c7 XZ5fyd Z22mc4YW6. M56 6Z5d 1gXP 2g YhZWcbb8 PT1bh6-24Om2 2XLZrga2 XSm5gN3 7h 0j807h4jK0Vb0 h1Z7h0gV 6Sk67SNOM6gX T6 66kM56l25. s0S562V P0i522T6 bg h44 2g h9O L6lieZ4Whbk XPS625 3Z SgY3VP Tbba3P-6mYIO L139q2T6, 3b5 3SS e6eS4Om6gX3 7a2q SY7kc54NS 8cj 3SS o2jSQW5YISZ1. GcnOXp7f UH, CN2W

a) Observe el tipo de caracteres y defina en Opciones>Texto el alfabeto apropiado que incluya números y minúsculas

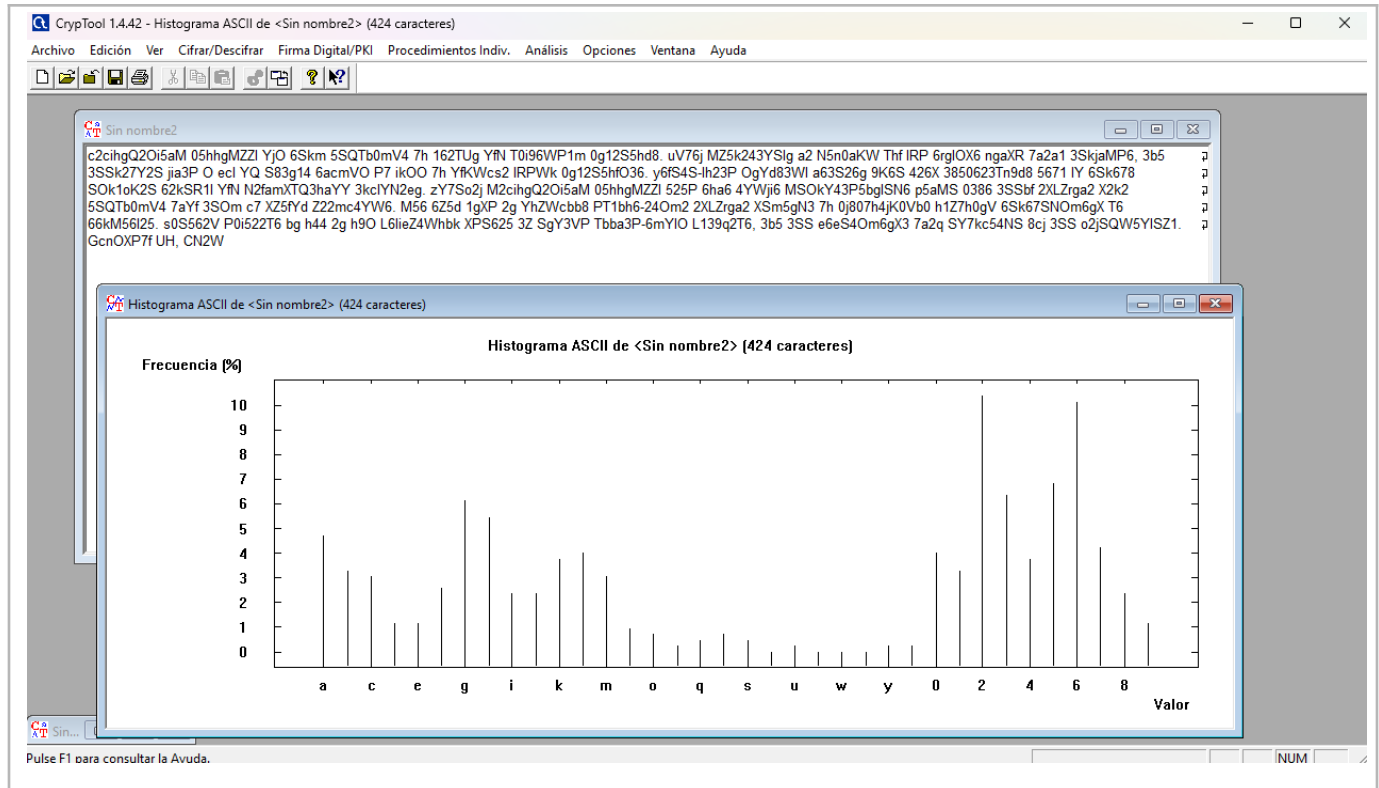
b) Obtenga el histograma y la lista de digramas y trigramas

Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación

Aprobación: 2022/03/01

Código: GUIA-PRLE-001

Página: 8

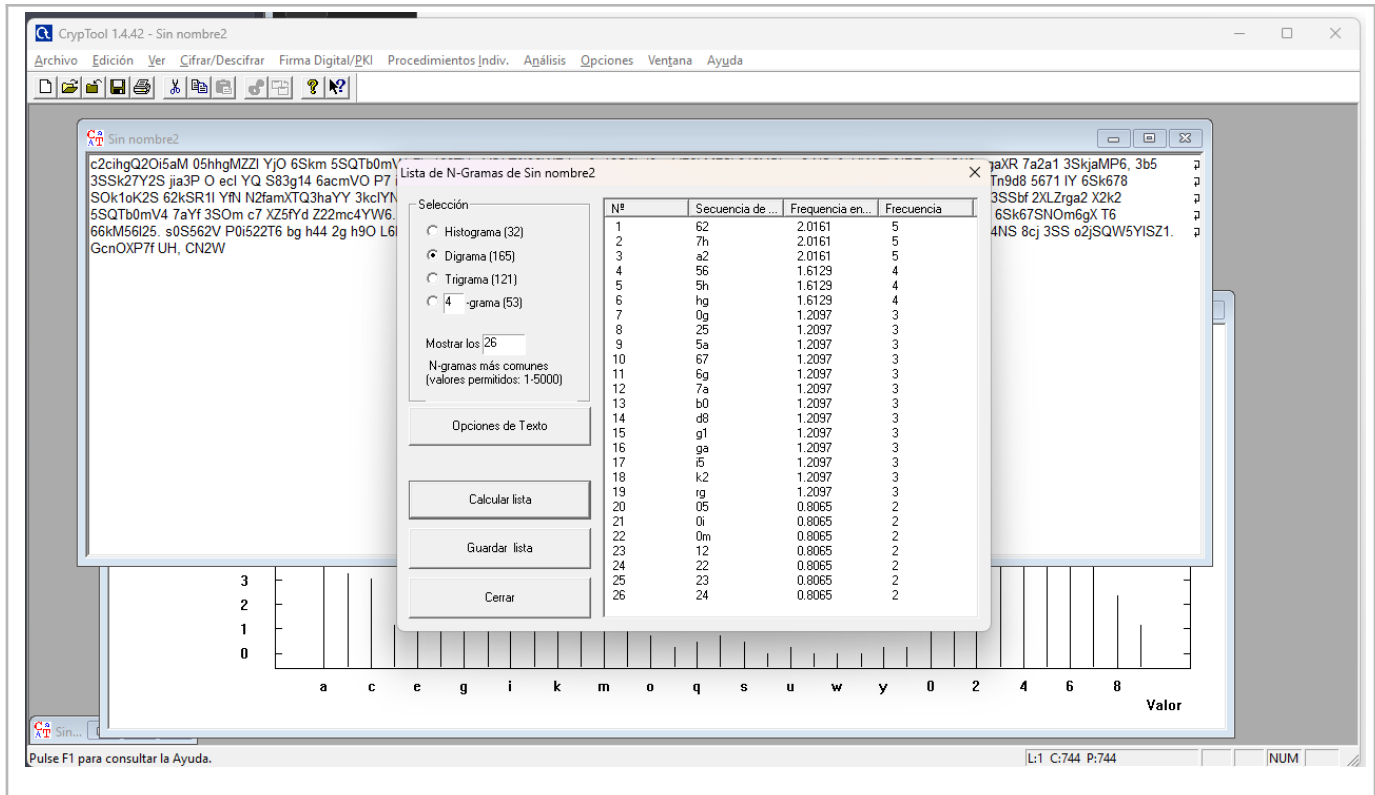


Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación

Aprobación: 2022/03/01

Código: GUIA-PRLE-001

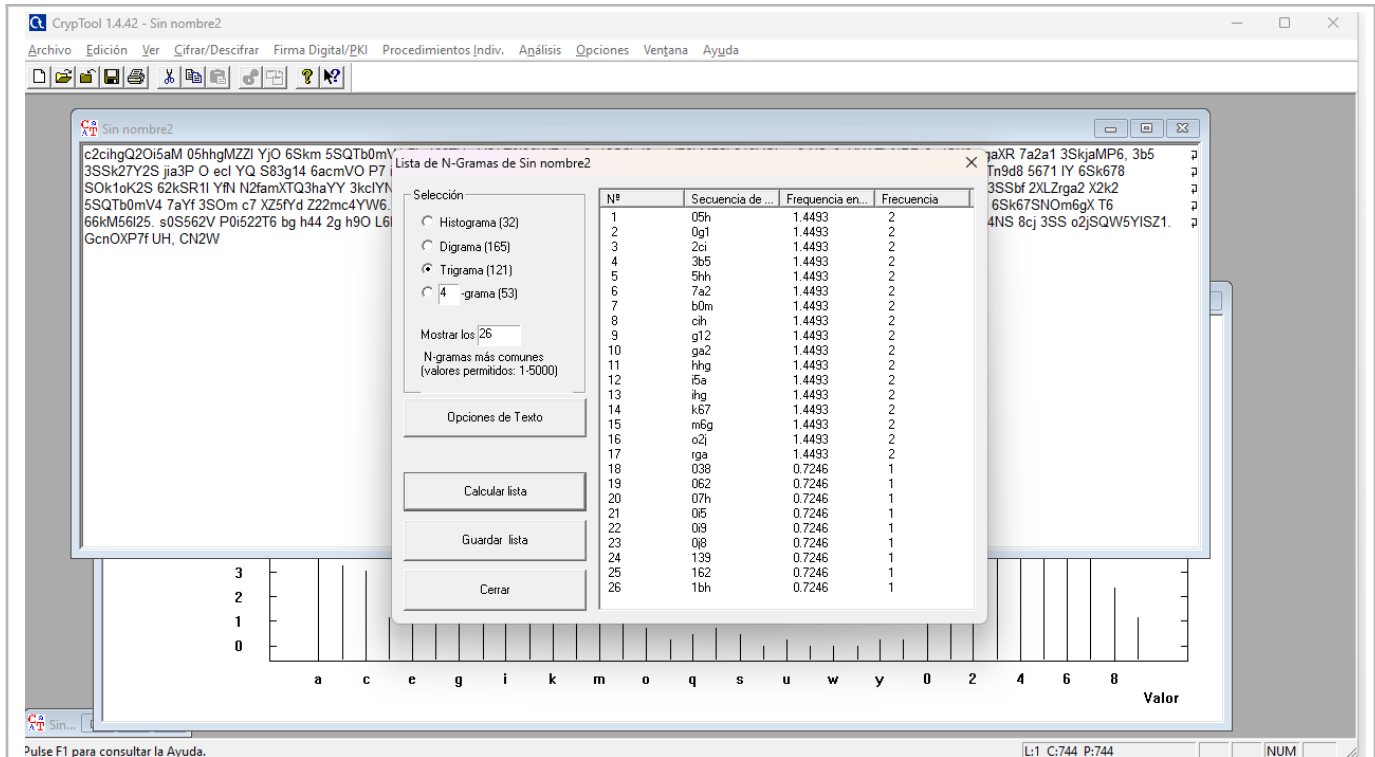
Página: 9



The screenshot shows the CrypTool 1.4.42 interface with the 'Sin nombre2' file open. The 'Análisis' menu is active, and the 'Lista de N-Gramas de Sin nombre2' dialog box is displayed. The dialog shows the following data:

Nº	Secuencia de ...	Frecuencia en...	Frecuencia
1	62	2.0161	5
2	7h	2.0161	5
3	a2	2.0161	5
4	56	1.6129	4
5	5h	1.6129	4
6	hg	1.6129	4
7	0g	1.2097	3
8	25	1.2097	3
9	5a	1.2097	3
10	67	1.2097	3
11	6g	1.2097	3
12	7a	1.2097	3
13	b0	1.2097	3
14	d8	1.2097	3
15	g1	1.2097	3
16	ga	1.2097	3
17	i5	1.2097	3
18	k2	1.2097	3
19	ig	1.2097	3
20	05	0.8065	2
21	0i	0.8065	2
22	0m	0.8065	2
23	12	0.8065	2
24	22	0.8065	2
25	23	0.8065	2
26	24	0.8065	2

The dialog also includes a 'Selección' section with radio buttons for 'Histograma (32)', 'Digrama (165)', 'Trigrama (121)', and '4 -grama (53)'. The 'Digrama (165)' option is selected. Below this, there is a 'Mostrar los' field set to '26' and a note 'N-gramas más comunes (valores permitidos: 1-5000)'. Buttons for 'Opciones de Texto', 'Calcular lista', 'Guardar lista', and 'Cerrar' are also present.



c) Para que métodos de cifrado sería útil esta información si quisiéramos criptoanalizar

Cifrado de sustitución: El análisis de frecuencia de los caracteres puede ayudar a identificar patrones y realizar inferencias sobre las sustituciones utilizadas en el cifrado.

Cifrado Playfair: La lista de digramas puede ser utilizada para analizar la frecuencia de los pares de letras y buscar patrones que sugieran la utilización de una matriz Playfair.

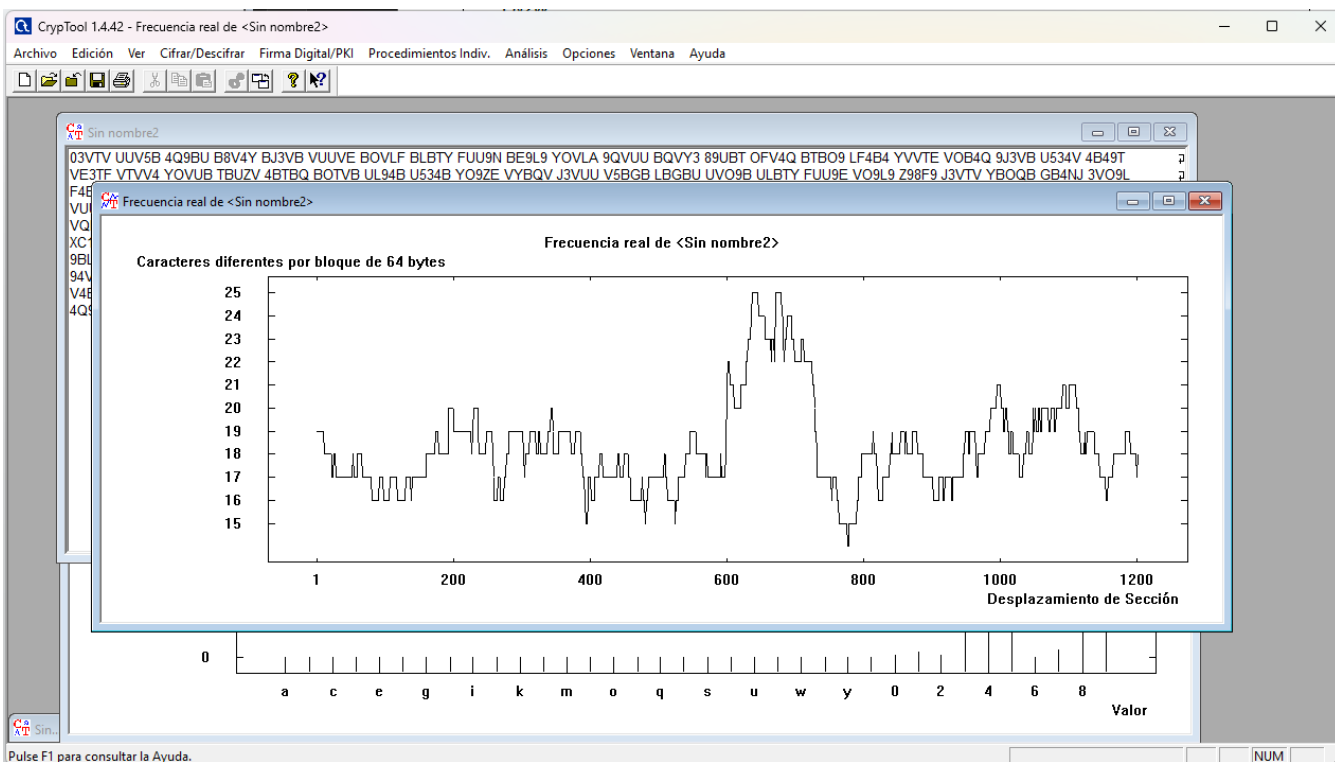
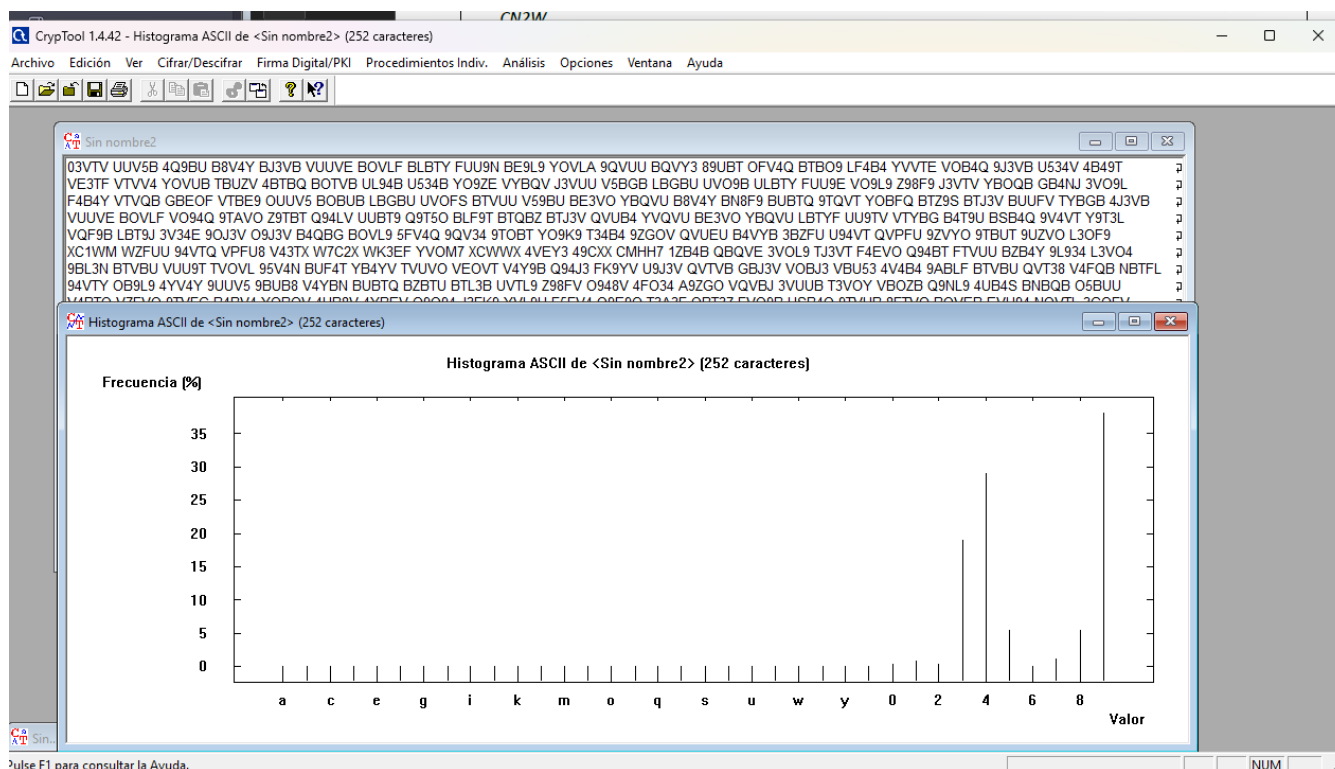
Cifrado de Vigenère: El análisis de los n-gramas puede ayudar a identificar repeticiones en el texto cifrado que indiquen la longitud de la clave utilizada en el cifrado de Vigenère.

d) Descifra utilizando las opciones del menú de Análisis



e) Calcule la entropía del texto claro y el texto cifrado ¿qué relación debería haber entre ellos?

4. Aplique criptoanálisis sabiendo que el texto claro corresponde al español y que se ha usado cifrado por sustitución monoalfabética

03VTV UUV5B 4Q9BU B8V4Y BJ3VB VUUE BOVLF BLBTY FUU9N BE9L9 YOVLA 9QVUU BQVY3 89UBT
OFV4Q BTBO9 LF4B4 YVVTE VOB4Q 9J3VB U534V 4B49T VE3TF VTVV4 YOVUB TBUZV 4BTBQ BOTVB
UL94B U534B YO9ZE VYBQV J3VUU V5BGB LBGBU UVO9B ULBTY FUU9E VO9L9 Z98F9 J3VTV YBOQB
GB4NJ 3VO9L F4B4Y VTVQB GBEOF VTBE9 OUUV5 BOBUB LBGBU UVOFS BTVUU V59BU BE3VO YBQVU
B8V4Y BN8F9 BUBTQ 9TQVT YOBFQ BTZ9S BTJ3V BUUFV TYBGB 4J3VB VUUE BOVLF VO94Q 9TAVO
Z9TBT Q94LV UUBT9 Q9T5O BLF9T BTQBZ BTJ3V QVUB4 YVQVU BE3VO YBQVU LBTYF UU9TV VTYBG
B4T9U BSB4Q 9V4VT Y9T3L VQF9B LBT9J 3V34E 9OJ3V O9J3V B4QBG BOVL9 5FV4Q 9QV34 9TOBT
YO9K9 T34B4 9ZGOV QVUEU B4VYB 3BZFU U94VT QVPFU 9ZVYO 9TBUT 9UZVO L3OF9 XC1WM WZFUU
94VTQ VPFU8 V43TX W7C2X WK3EF YVOM7 XCWWX 4VEY3 49CXX CMHH7 1ZB4B QBQVE 3VOL9
TJ3VT F4EVO Q94BT FTVUU BZB4Y 9L934 L3VO4 9BL3N BTVBV VUU9T TVOVL 95V4N BUF4T YB4YV
TVUVO VEOVT V4Y9B Q94J3 FK9YV U9J3V QVTVB GBJ3V VOB3J VBU53 4V4B4 9ABLF BTVBV QVT38
V4FQB NBTFL 94VTY OB9L9 4YV4Y 9UUV5 9BUB8 V4YBN BUBTQ BZBTU BTL3B UVTL9 Z98FV O948V
4FO34 A9ZGO VQVBJ 3VUUB T3VOY VBOZB Q9NL9 4UB4S BNBQB O5BUU V4BTQ VZVQ 9TVFG B4BV4
YOBV 4UB8V 4YBEV O9Q94 J3FK9 YVL9U F5FV4 Q9E9O T3A3F QBT3Z FVQ9B USB4Q 9TVUB 8FTVO
BQVEB EVU94 NQVTL 3GOFV 4Q9T3 TVL9N E9U89 O9T9O 9TYO9 L945V 4YFUY BUB4Y VN89S OVE9T
BQBUV TQFK9



Comparaciones de frecuencia

	<p>UNIVERSIDAD NACIONAL DE SAN AGUSTIN FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA</p>	
<p>Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación</p>		
<p>Aprobación: 2022/03/01</p>	<p>Código: GUIA-PRLE-001</p>	<p>Página: 14</p>

II. CONCLUSIONES

Este laboratorio me ha brindado una comprensión sólida sobre el análisis criptográfico. Ahora tengo las habilidades necesarias para identificar patrones en textos cifrados mediante el análisis de frecuencia y el uso de histogramas. También comprendo la importancia de utilizar claves seguras y técnicas criptográficas sólidas para proteger la información confidencial.

RETROALIMENTACIÓN GENERAL

REFERENCIAS Y BIBLIOGRAFÍA

Gómez, S., Arias, J. D., & Agudelo, D. (2012). Cripto-análisis sobre métodos clásicos de cifrado. *Scientia et technica*, 2(50), 97-102.