

# Laboratorio #3

Cifrado Elemental

**Alumna:** Chullunquía Rosas, Sharon Rossely Alisson

**Docente:** Franklin Luis Antonio Cruz Gamero

**Fecha:** 26 de septiembre de 2021

Arequipa, Perú

# Índice de Contenidos

1. Actividades	1
2. Conclusiones	15
3. Cuestionario Final	16
Referencias	18

# Índice de Figuras

1. Cifrado con clave 'a'	1
2. Cifrado con clave 'A'	1
3. Cifrado con clave 'z'	2
4. Cifrado con clave '3'	2
5. Alineación de alfabetos con la clave 'a'	3
6. Alineación de alfabetos con la clave 'A'	3
7. Alineación de alfabetos con la clave 'z'	4
8. Alineación de alfabetos con la clave '3'	4
9. Caracteres que se pueden agregar	5
10. Cifrado Playfair con la palabra clave 'CONSUL'	6
11. Matriz 5x5	6
12. Pre-formateo de Playfair	7
13. Descifrado con algoritmo Playfair	7
14. Matriz de 6x6	8
15. Cifrado con matriz de 6x6	8
16. Definiendo alfabeto apropiado e incluyendo números y minúsculas	9
17. Histograma	10
18. Lista de digramas	10
19. Lista de trigramas	11
20. Clave encontrada	11
21. Descifrado	12
22. Entropía del texto cifrado	12
23. Entropía del texto descifrado	13
24. Texto descifrado con Afin	14
25. Análisis de frecuencias en histograma	16
26. Cifrado con Multiplicative	17
27. Cifrado con Gronsfield	17

# 1. Actividades

## 1. Sea el texto claro

*La criptografía Simétrica es un método criptográfico monoclave, esto quiere decir que se usa la misma clave para cifrar y descifrar. Esto supone un grave problema a la hora de realizar el intercambio entre el emisor y el receptor, dado que si una tercera persona estuviese escuchando el canal podría hacerse con la clave, siendo inútil el cifrado. Es importante que la clave sea difícil de adivinar y el método de cifrado empleado el adecuado. Hoy en día, con la capacidad computacional disponible, si se emplean los algoritmos adecuados, dependiendo del método de cifrado empleado se puede obtener una clave en cuestión de minutos-horas.*

- a) Cifre utilizando el algoritmo de Cesar, eligiendo un alfabeto que contenga mayúsculas y minúsculas, utilice las siguientes claves 'a', 'A', 'z', '3'

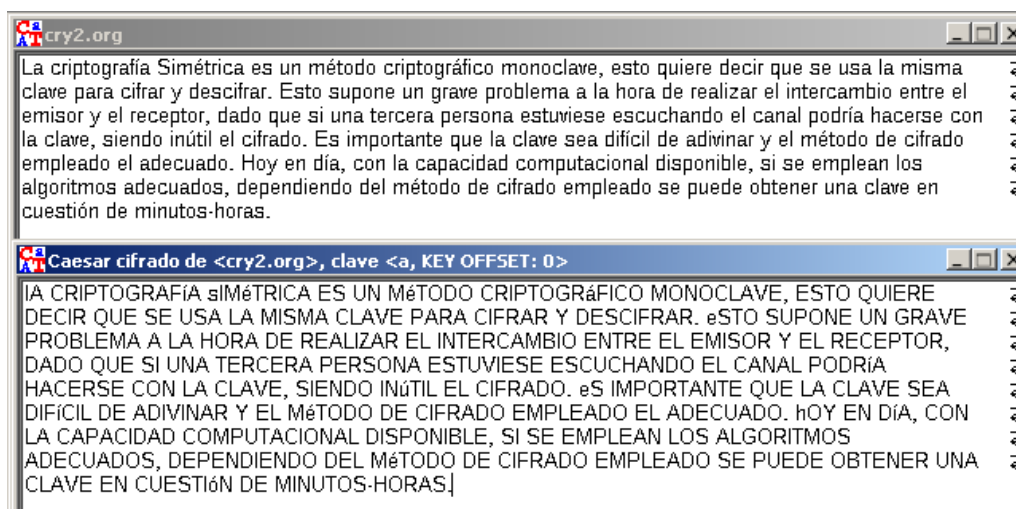


Figura 1: Cifrado con clave 'a'

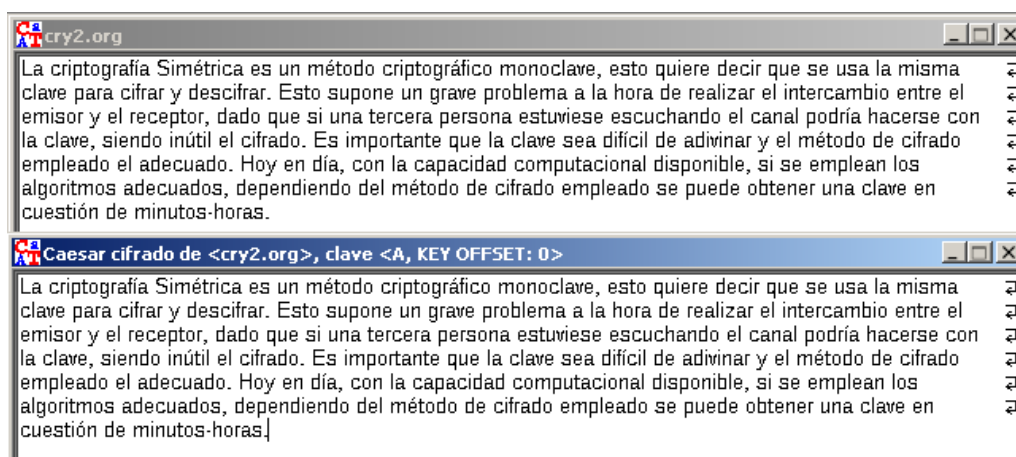


Figura 2: Cifrado con clave 'A'

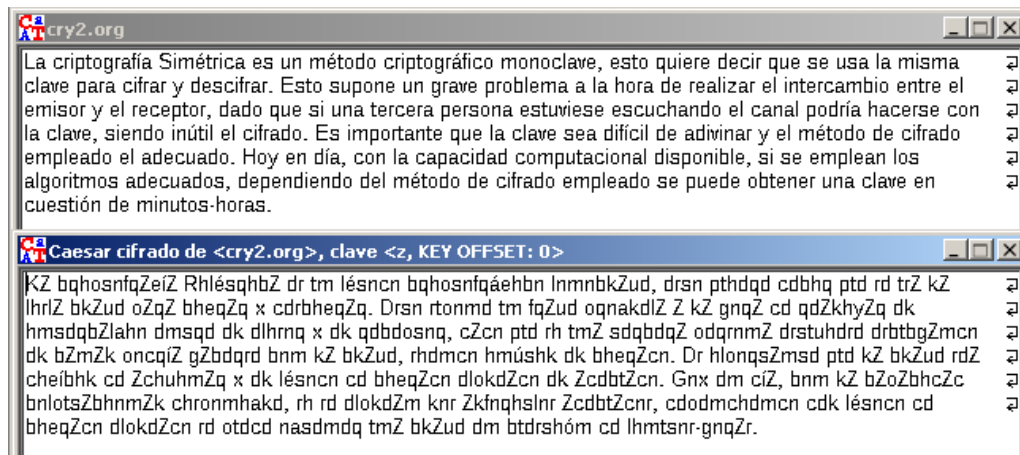


Figura 3: Cifrado con clave 'z'

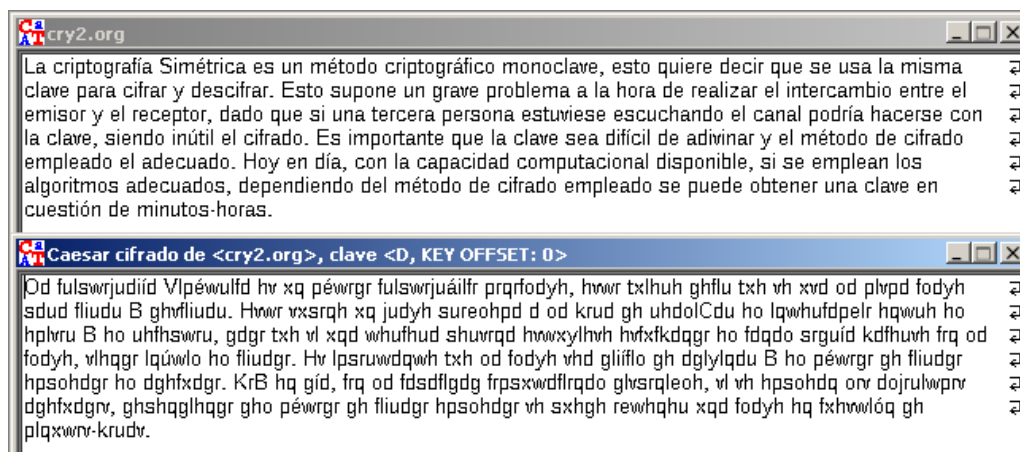



Figura 4: Cifrado con clave '3'

### b) Explique los resultados obtenidos

Para los resultados obtenidos, se usó el algoritmo de César. Este consiste en escoger una letra del texto plano y otra del alfabeto escogido, después se aplica el módulo para la alineación de los alfabetos, y finalmente se realiza una sustitución directa. (Stallings, Brown, Bauer, y Bhattacharjee, 2012)

En el caso de la figura 1, se observa en el texto cifrado que aquellas letras que eran mayúsculas en el texto plano, son minúsculas; y las letras minúsculas, son mayúsculas. Esto es porque existe una alineación entre el alfabeto en mayúsculas y el alfabeto en minúsculas (Ver figura 5) por la clave 'a' ingresada.

Introducir clave como

☒ Caracter del alfabeto  

☐ Valor Numérico

Propiedades del cifrado elegido

Cambio de 26

Mapa de caracteres del alfabeto (52 caracteres)


de:

a:

Figura 5: Alineación de alfabetos con la clave 'a'

En el cifrado con clave 'A', el texto plano es idénticamente al texto cifrado, ya que la alineación los alfabetos coinciden en el mismo carácter (Ver figura 6).

Introducir clave como

☒ Caracter del alfabeto  

☐ Valor Numérico

Propiedades del cifrado elegido

Cambio de 0

Mapa de caracteres del alfabeto (52 caracteres)


de:

a:

Figura 6: Alineación de alfabetos con la clave 'A'

En el cifrado con clave 'z', el alfabeto se alinea con el otro alfabeto pero iniciando con el carácter de la clave (Ver figura 7). Por lo que en el cifrado, cada carácter es recorrido en una posición.

Introducir clave como

☒ Caracter del alfabeto  

☐ Valor Numérico

---

Propiedades del cifrado elegido

Cambio de 51

Mapa de caracteres del alfabeto (52 caracteres)


de:

a:

Figura 7: Alineación de alfabetos con la clave 'z'

Cuando ciframos con la clave '3', el cifrado de cada carácter recorre en 3 posiciones (Ver figura 8), debido a eso, es que el segundo alfabeto recorre en 3 posiciones, empezando en 'D'.

Introducir clave como

☐ Caracter del alfabeto  

☒ Valor Numérico

---

Propiedades del cifrado elegido

Cambio de 3

Mapa de caracteres del alfabeto (52 caracteres)

de:

a:

Figura 8: Alineación de alfabetos con la clave '3'

c) **¿Qué otros caracteres puede añadir al alfabeto?**

Además de letras mayúsculas y minúsculas, se puede agregar espacios, puntuación (ej. \.,,:;! ?()-+\* /[]{}@ \\_><#~=\ "& \ % \$), caracteres con diéresis (ej. Ä Ö Ü ä ö ü) y números (ej. 0123456789).

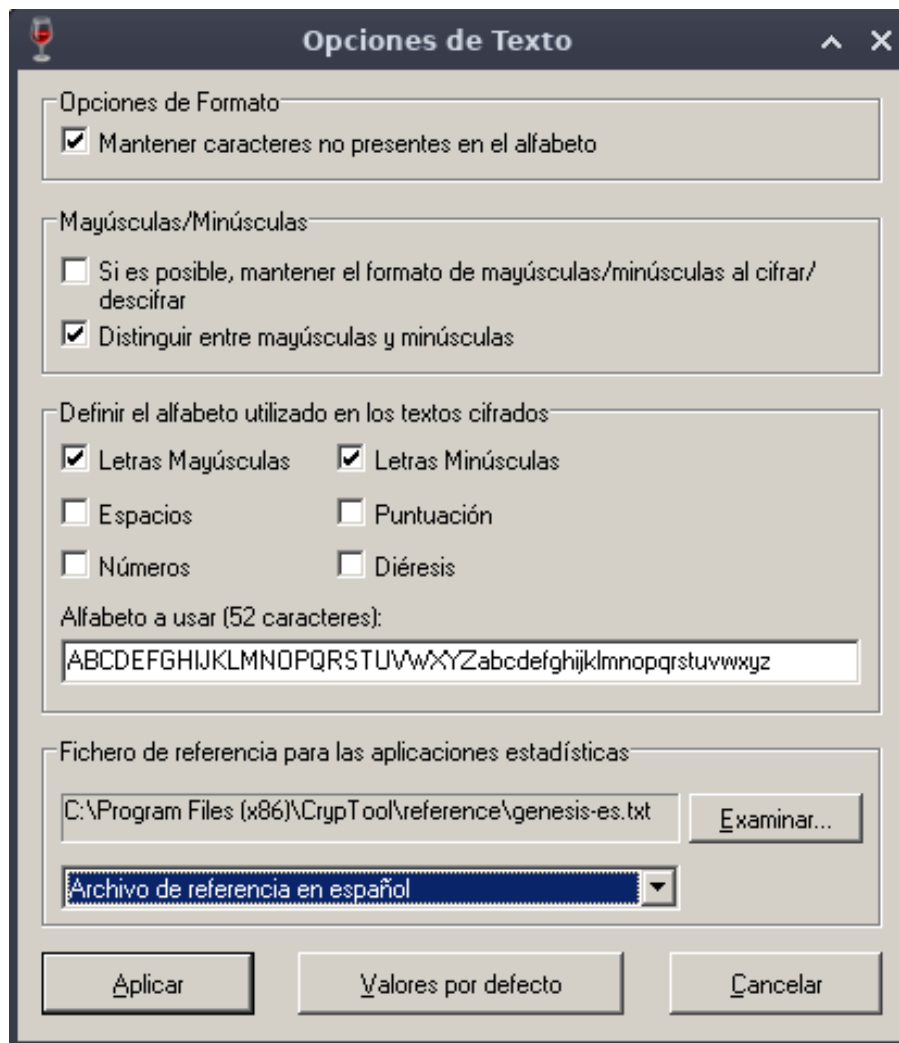


Figura 9: Caracteres que se pueden agregar

## 2. Sea el texto claro

*Para cifrar archivos y carpetas con criptografía simétrica existen varias tecnologías. Es conveniente consultar la especificación de cada herramienta para determinar si es capaz de proveer la seguridad que se requiere. Una de las herramientas gratuitas, multiplataforma que es capaz de proveer un fuerte cifrado AES de 256 bits es 7zip. Winzip y Winrar proveen también cifrado AES, en sus versiones actuales. Para cifrar un archivo o carpeta con estas herramientas, es necesario ir al apartado de seguridad y establecer una contraseña. En caso de que se pregunte, seleccionar el algoritmo y la longitud de preferencia del usuario, con base en las necesidades de seguridad que desee implementar.*

- a) Cifre utilizando el algoritmo de Playfair, usando una matriz 5x5 con la clave CONSUL, explique la matriz clave

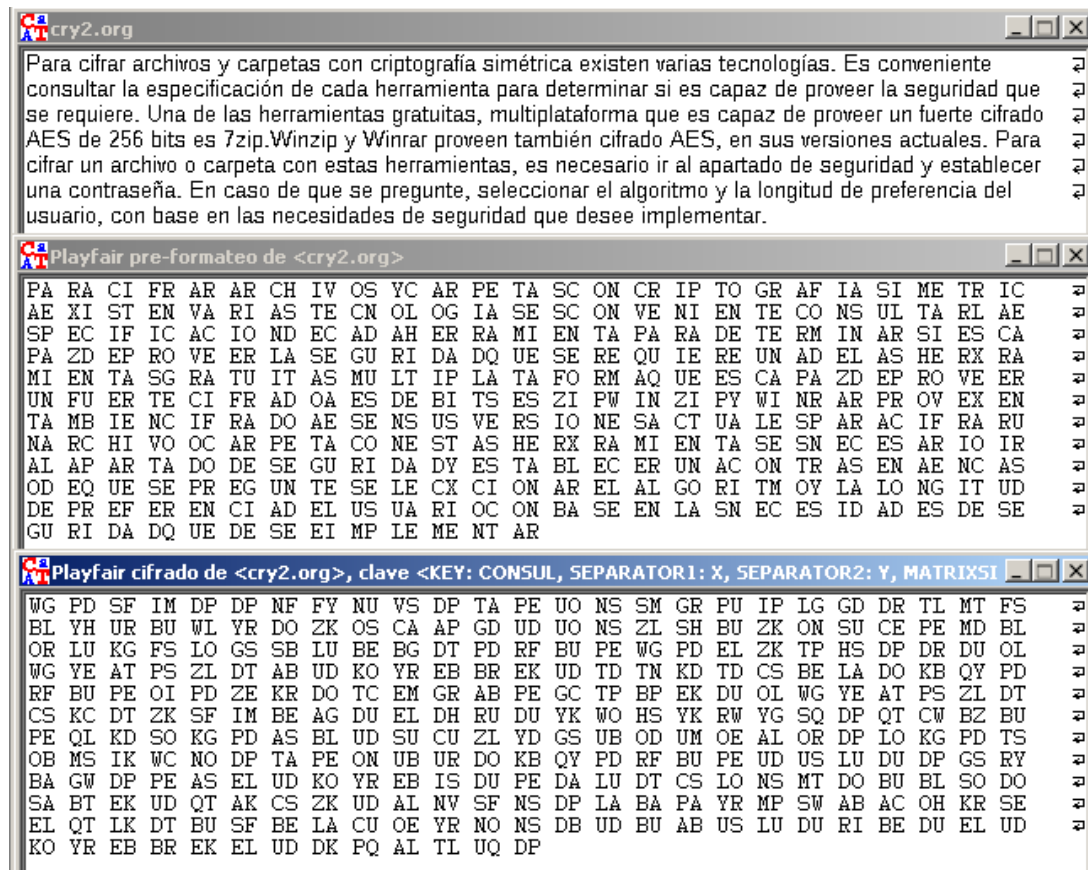


Figura 10: Cifrado Playfair con la palabra clave 'CONSUL'

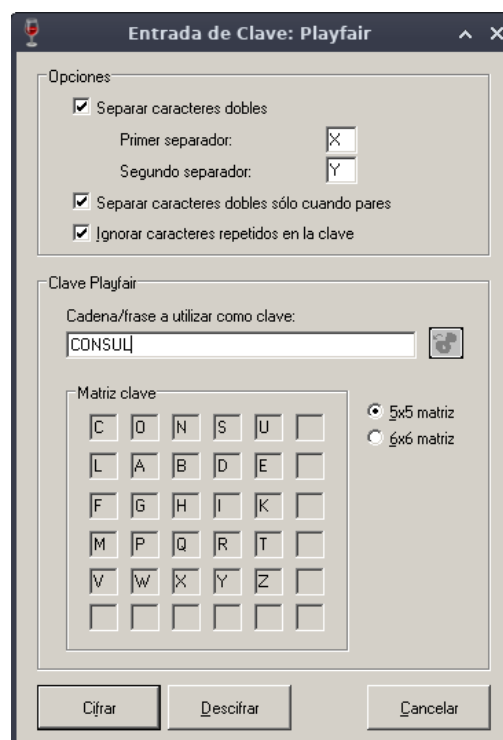


Figura 11: Matriz 5x5



En la matriz clave de 5x5 (Ver figura 11), se observa que en la primera fila se encuentra la palabra clave 'CONSUL', a excepción de su último carácter, ya que este pasa a la segunda fila, porque la matriz es de 5x5 y la palabra 'CONSUL' tiene 6 caracteres. Después de la palabra clave en la matriz, sigue el alfabeto de los caracteres en mayúsculas, pero sin contar las letras de la palabra clave 'CONSUL' y la letra 'J', la cual no es contada en el algoritmo de Playfair desde un inicio.

b) **Explique el resultado mostrado en el pre-formateo**

En el resultado del pre-formateo, se observa que todos los caracteres pasaron a ser mayúscula y fueron divididos en digramas (Ver figura 12).

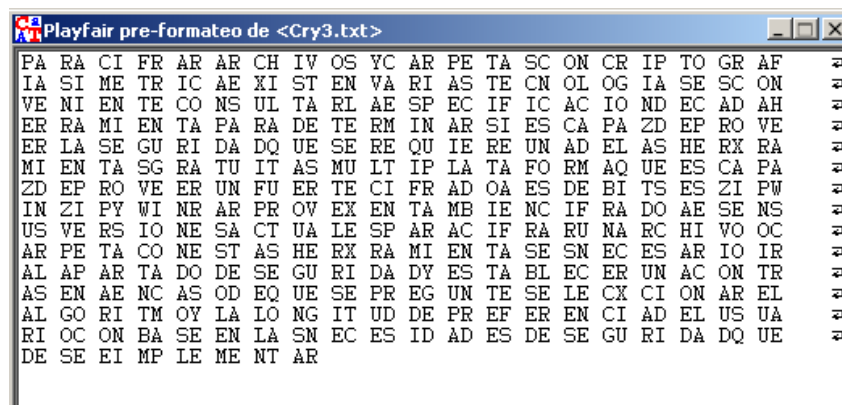


Figura 12: Pre-formateo de Playfair

c) **Descifre el resultado explique lo que se obtiene**

El resultado del descifrado es el mismo al del pre-formateo del texto plano, cuando se realiza el cifrado. El descifrado esta todo en mayúsculas y separado en digramas.



Figura 13: Descifrado con algoritmo Playfair

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

En el cifrado con matriz 6x6, la matriz ya no solo considera la palabra clave y el alfabeto en mayúsculas, incluye también números (Ver figura 14).

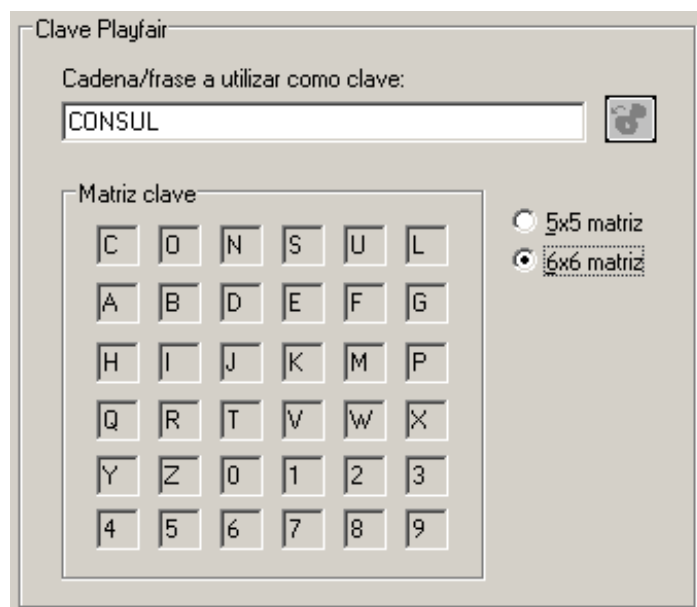


Figura 14: Matriz de 6x6

Cuando se cifra con una matriz de 5x5, todos los caracteres son del alfabeto en mayúsculas, sin embargo, cuando ciframos con una matriz de 6x6, se encuentra nuevos caracteres en el texto cifrado. Estos nuevos caracteres son números (Ver figura 15).

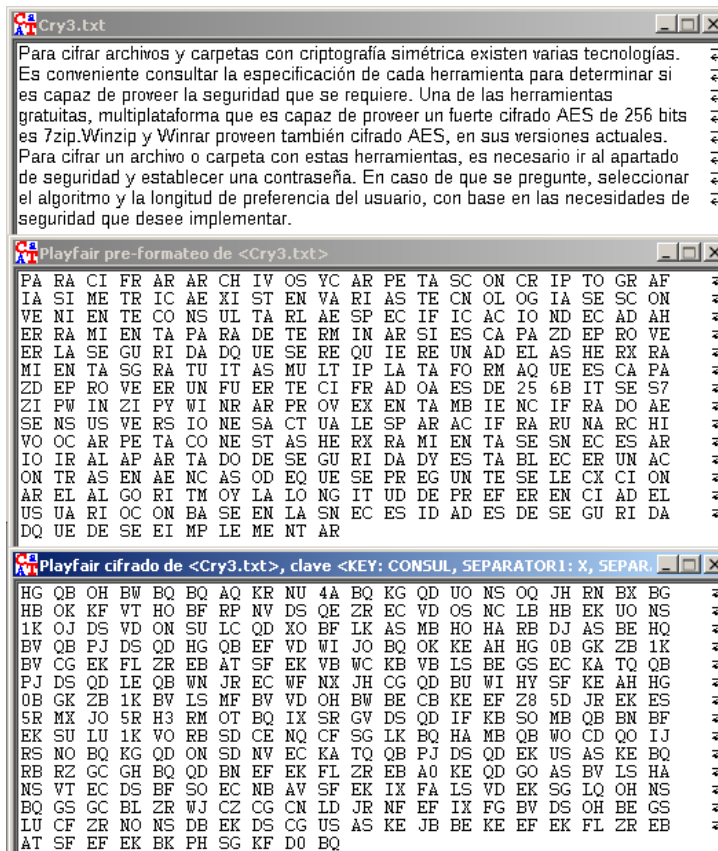


Figura 15: Cifrado con matriz de 6x6

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

*c2cihgQ2Oi5aM 05hhgMZZl YjO 6SkM 5SQTb0mV4 7h 162TUg YfN T0i96WP1m  
0g12S5hd8. uV76j MZ5k243YSlg a2 N5n0aKW Thf lRP 6rglOX6 ngaXR 7a2a1 3Sk-  
jaMP6, 3b5 3SSk27Y2S jia3P O ecl YQS83g14 6acmVO P7 ikOO 7h YfKWcs2  
lRPWk 0g12S5hfO36. y6fS4S-lh23P OgYd83Wl a63S26g 9K6S 426X 3850623Tn9d8  
5671 lY 6Sk678 SOk1oK2S 62kSR1l YfN N2famXTQ3haYY 3kclYN2eg. zY7So2j  
M2cihgQ2Oi5aM 05hhgMZZl 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 L6lieZ4  
Whbk XPS625 3Z SgY3VP Tbba3P-6mYlO L139q2T6, 3b5 3SS e6eS4Om6gX3 7a2q  
SY7kc54NS 8cj 3SS o2jSQW5YlSZ1. GcnOXP7f UH, CN2W*

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

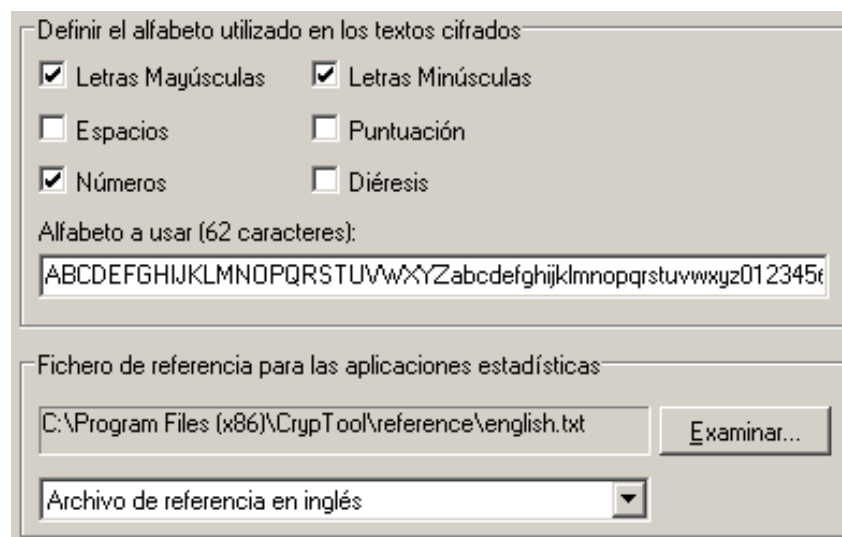


Figura 16: Definiendo alfabeto apropiado e incluyendo números y minúsculas

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

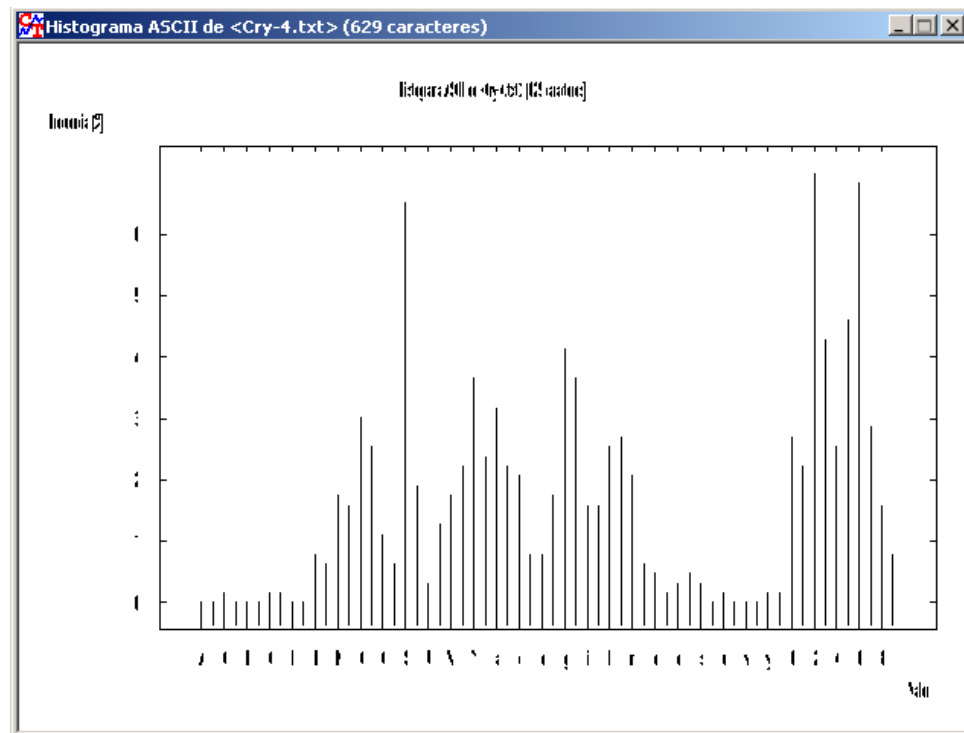


Figura 17: Histograma

Lista de N-Gramas de Cry-4.txt

Selección

☐ Histograma (51)

☒ Digrama (348)

☐ Trigrama (363)

☐ 4 -grama (295)

Mostrar los 26

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

Opciones de Texto

Calcular lista

Guardar lista

Cerrar

Nº	Secuencia d...	Frecuencia e...	Frecuencia
1	3S	1.3359	7
2	62	0.9542	5
3	7h	0.9542	5
4	Sk	0.9542	5
5	a2	0.9542	5
6	2S	0.7634	4
7	3P	0.7634	4
8	56	0.7634	4
9	5h	0.7634	4
10	6S	0.7634	4
11	Om	0.7634	4
12	SS	0.7634	4
13	Yi	0.7634	4
14	aM	0.7634	4
15	hg	0.7634	4
16	0g	0.5725	3
17	25	0.5725	3
18	2T	0.5725	3
19	5a	0.5725	3
20	67	0.5725	3
21	6g	0.5725	3
22	7a	0.5725	3
23	MZ	0.5725	3
24	N2	0.5725	3
25	S5	0.5725	3
26	SO	0.5725	3

Figura 18: Lista de digramas

Nº	Secuencia d...	Frecuencia e...	Frecuencia
1	3SS	0.9524	4
2	5aM	0.7143	3
3	6Sk	0.7143	3
4	05h	0.4762	2
5	0g1	0.4762	2
6	0mV	0.4762	2
7	12S	0.4762	2
8	20i	0.4762	2
9	2S5	0.4762	2
10	2T6	0.4762	2
11	2XL	0.4762	2
12	2ci	0.4762	2
13	3b5	0.4762	2
14	40m	0.4762	2
15	4Yw	0.4762	2
16	5SQ	0.4762	2
17	5hh	0.4762	2
18	6gX	0.4762	2
19	7a2	0.4762	2
20	LZr	0.4762	2
21	M56	0.4762	2
22	MZZ	0.4762	2
23	Oi5	0.4762	2
24	Om6	0.4762	2
25	Q20	0.4762	2
26	QTb	0.4762	2

Figura 19: Lista de trigramas

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

Para aquellos métodos que hacen uso del cifrado simétrico clásico, o los de sustitución. El método de Vigenere es un ejemplo.

- d) Descifre utilizando las opciones del menú de Análisis

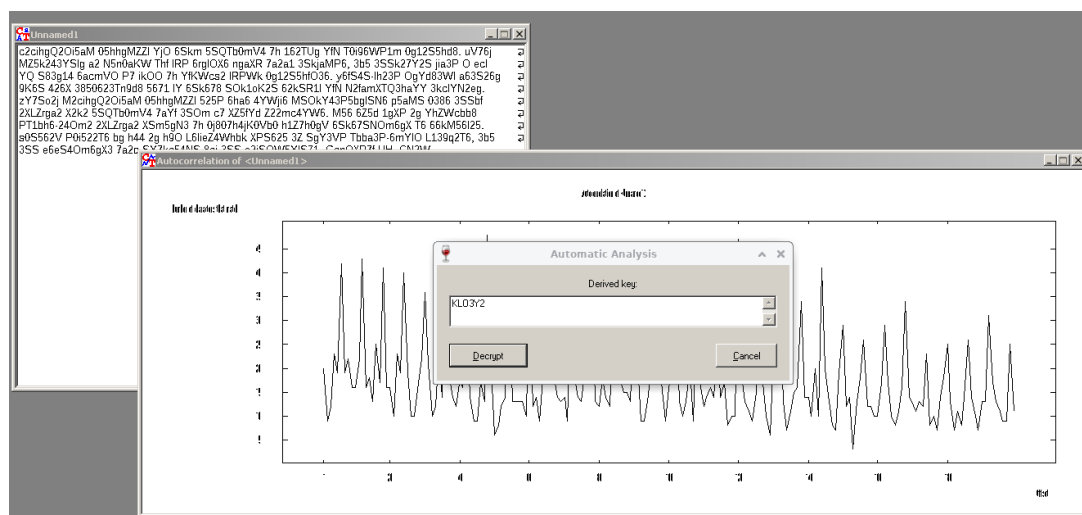


Figura 20: Clave encontrada

## Vigenère

Cipher Description Background Security About alphabets

**Plaintext:**

SrOptoGrApHiC protoCOLs krE vEry DIFFiCult to DEsIGN knD ImPLEment CorrECtly. jHEir CORrECtNEss is CruCiAL For the systEMs using thEir sErviCEs, AnD tHEReFORe quite A lot OF Effort shouLD BE usED to knALoZE tHEir CorrECtnEss. 5InItE-stAtE AnklysIs mEtHoDs HAVe BEEN suCCEssFuLly usED tO vERiFY HARdWArE DESIGns knD CommuNICAtION protoCOLs. 7OwEvEr CrOptoGrApHiC protoCOLs HAVe somE uNIquE CHArKtErIsTICs wHiCH MAKE tHEir ANALySis MorE DIFFiCult thkn tHAT OF NOrmkl ProtoCOLs. THE wOrk DoNE on kpPLöInG FinitE-stAtE ANALySis METHoDs to CryptoGrApHiC prOtocol vErIFICAtIoN Is DISCussED. ipECIAL EmPHASIs is put on tHE AssumPtions NEEDED tO EnkBLE FinitE-stktE AnALySis, AnD tHE lImItAtIoNs thEy INtroDuce For tHE vERiFICtIoN. NovEMBER c7, 199i

Figura 21: Descifrado

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

The screenshot shows a text editor window titled 'Unnamed1' containing a ciphertext. Below the text, a dialog box titled 'Entropy <Unnamed1>' is displayed. The dialog box contains the following text:

This document contains 51 different characters compared to the 62 characters of the selected alphabet.

**The entropy of the whole document is 5.16 (maximum possible entropy 5.95).**

OK

Figura 22: Entropía del texto cifrado

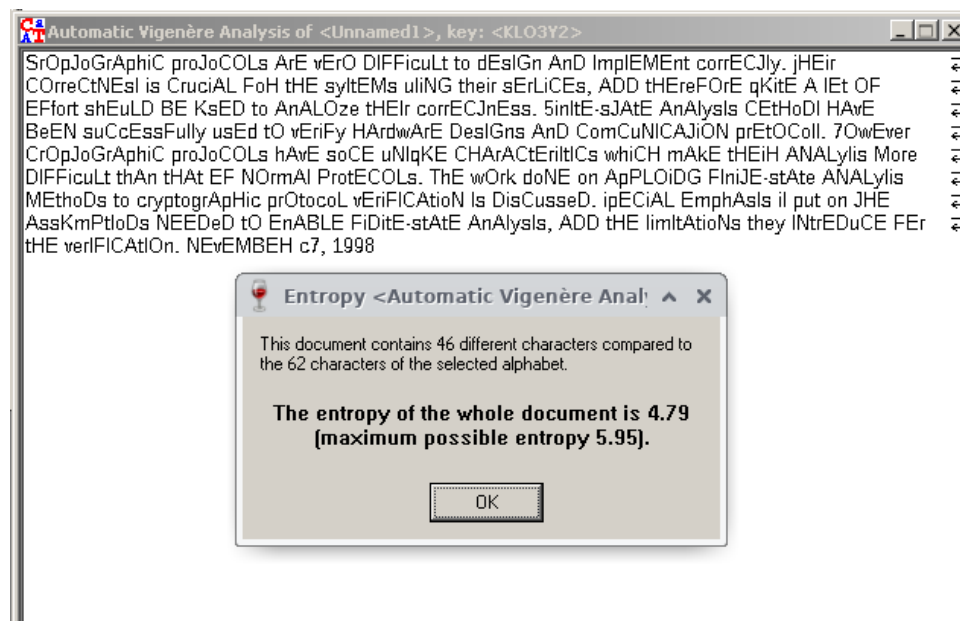


Figura 23: Entropía del texto descifrado

La entropía para el texto cifrado es 5.16 y para el texto descifrado es 4.79. La entropía es casi la misma, se aproximan bastante. Sin embargo, en la máxima entropía coinciden en el mismo número.

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

03VTV UUV5B 4Q9BU B8V4Y BJ3VB VUUE BOVLF BLBTY FUU9N BE9L9  
 YOVL9 9QVUU BQVY3 89UBT OFV4Q BTBO9 LF4B4 YVVTE VOB4Q 9J3VB  
 U534V 4B49T VE3TF VTVV4 YOVL9 TBVZV 4BTBQ BOTVB UL94B U534B  
 YO9ZE VYBQV J3VUU V5BGB LBGBU UVO9B ULBTY FUU9E VO9L9 Z98F9  
 J3VTV YBOQB GB4NJ 3VO9L F4B4Y VTVQB GBEOV VTBE9 OUUV5 BO-  
 BUB LBGBU UVOFS BTVUU V59BU BE3VO YBQVU B8V4Y BN8F9 BUBTQ  
 9TQVT YOBFB 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 9UZ-  
 VO 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  
 VZFBV 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

Usando el descifrado Afin con 36 letras, con decimación de 5 y desplazamiento de 1, se obtiene lo siguiente:

**Afin Z36**

Cifrar Descifrar Clave Ayuda contextual Cargar: Ejemplo de prueba

Entrada: OB9L9 4YV4Y 9UUV5 9BUB8 V4YBN BUBTQ BZBTU BTL3B UVTL9 Z98FV O948V 4FO34 A9ZGO VQVBJ 3VUUB T3VOY VBOZB Q9NL9 4UB4S BNBQB O5BUU V4BTQ VZFBQ 9TVFG B4BV4 YOB0V 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

Fichero entrada: Fichero

Salida: FUESELLEGANDOALAVENTAQUEAELELPARECIACASTILLOYAPOCOTRECHODELLADETUVOLASRIEN DASAROCINANTEESPERANDOQUEALGUNENANOSEPUSIESEENTRELASALMENASADARSEALCONAL GUNATROMPETADEQUELEGABACABALLEROALCASTILLOPEROCOMOVIOQUESETARDABANYQUE ROCINANTESEDABAPRIESAPORILLEGARALACABALLERIZASELLEGOALAPUERTADELAVENTAYVIOALA SDOSDESTRAIDASMOZASQUEALLIESTABANQUEAELELPARECIERONDOSHERMOSASDONCELLASO

Fichero salida: Fichero

Preparado 100%

Figura 24: Texto descifrado con Afin



## 2. Conclusiones

- Se puede descriptar haciendo uso del análisis mediante la correlación, incluso sin tener la clave, ya que con el análisis del texto cifrado, se puede obtener el tamaño de la clave y la clave misma.
- Una baja entropía es un claro indicio de que el criptosistema puede ser vulnerado, dando una mayor probabilidad de poder predecir los valores generados.
- Para una fácil correlación de las letras entre el texto cifrado y el texto plano, sirven de ayuda las listas de digramas, trigramas y la frecuencia de letras.
- El cifrado simétrico usa la misma clave para cifrar y descifrar, por lo que se deduce que es de tipo monoclave.
- Operaciones como la obtención de n-gramas, histogramas y el análisis de frecuencias en el texto cifrado, nos hace posible el criptoanálisis.
- Aquellos algoritmos que son por sustitución monoalfabética pueden descifrarse con el análisis de frecuencia.
- La frecuencia de las letras del idioma del texto cifrado nos son de gran ayuda a la hora de realizar el criptoanálisis.
- No son recomendables los sistemas de cifrado monográficos, ya que genera bastante redundancia en sus criptogramas y en el texto en claro, haciendo muy evidente el criptoanálisis.

### 3. Cuestionario Final

#### 1. Defina el concepto de entropía

La entropía es una medida de la aleatoriedad de una función generadora de datos. Los datos con entropía son del todo aleatorios y difíciles de encontrar en ellos, patrones significativos (Edgar y Manz, 2017). Si no hay una buena entropía, puede dejar el criptosistema incapaz de cifrar datos de forma segura (Wagner, 2020). Los datos con baja entropía generan la probabilidad de predecir los próximos valores generados, vulnerando así el criptosistema. (Edgar y Manz, 2017)

Para los algoritmos criptográficos, la entropía también es fundamental, ya que se usa para la generación de entradas aleatorias como, vectores de inicialización, claves, etc. Estos valores tienen que ser secretos, no predecibles, con el fin de garantizar seguridad en el proceso. Por tal motivo, es crucial contar con fuentes de datos de alta entropía por seguridad. Ejemplos de fuentes comunes de entropía son, la entrada del teclado/mouse, el voltaje de un circuito y las lecturas térmicas. (Edgar y Manz, 2017)

#### 2. ¿Qué información se puede obtener del histograma?

El histograma nos proporciona un análisis de las frecuencias de caracteres. Ya sea frecuencias de trigramas o digramas, mediante el uso de caracteres frecuentes del idioma del texto cifrado,

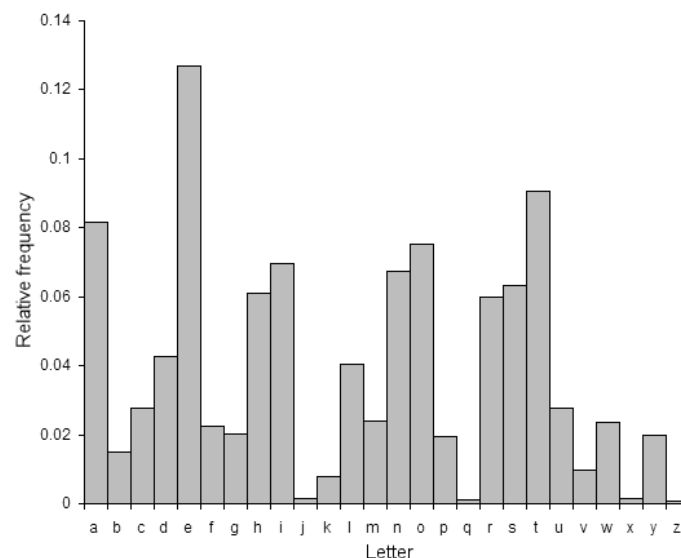


Figura 25: Análisis de frecuencias en histograma

#### 3. Describa los códigos Base 64 y UU

Base64 es un conjunto de esquemas de codificación de binario a texto, que simbolizan datos binarios en un formato de cadena ASCII, realizando la traducción a radix-64. Los códigos Base 64 son originados de una codificación de transferencia de contenido MIME específico. (Docs, s.f.) Los esquemas de codificación Base64 se usan comúnmente cuando existe la necesidad de codificar datos binarios que deben almacenarse

y transferirse a través de medios diseñados para tratar con ASCII. UUEncode es una herramienta de encriptación simétrica que encripta en bloques de código binario, que normalmente son códigos de 6 bits, para luego convertirlo a caracteres ASCII.(Sheppard y Carter, 1993)

#### 4. Repita el ejercicio 2 usando al menos otras dos técnicas de cifrado

**Texto plano:** *En las noches claras, resuelvo el problema de la soledad del ser.*

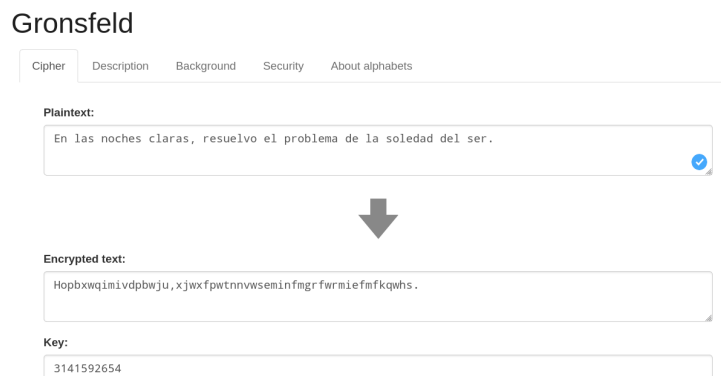
##### ■ Multiplicative



The screenshot shows the 'Multiplicative' cipher tool interface. It has a title bar 'Multiplicative' and four tabs: 'Cipher', 'Description', 'Security', and 'About alphabets'. The 'Cipher' tab is active. Under 'Plaintext:', there is a text input field containing 'En las noches claras, resuelvo el problema de la soledad del ser.' with a blue checkmark icon on the right. A large downward arrow points to the 'Encrypted text:' section, which contains a text output field with the encrypted text 'Qn fau neipqu ifadau, dqucqfte qf vderfqwa zq fa uefqzaz zqf ugd.'. Below this is an 'Options:' section with a 'Multiplier:' dropdown menu set to '17'.

Figura 26: Cifrado con Multiplicative

##### ■ Gronsfeld



The screenshot shows the 'Gronsfeld' cipher tool interface. It has a title bar 'Gronsfeld' and five tabs: 'Cipher', 'Description', 'Background', 'Security', and 'About alphabets'. The 'Cipher' tab is active. Under 'Plaintext:', there is a text input field containing 'En las noches claras, resuelvo el problema de la soledad del ser.' with a blue checkmark icon on the right. A large downward arrow points to the 'Encrypted text:' section, which contains a text output field with the encrypted text 'Hopbxwqimivdpbwju,xjwxfpwtnnvwseinfmgrfwrmiiefmfkqwhs.'. Below this is a 'Key:' section with a text input field containing '3141592654'.

Figura 27: Cifrado con Gronsfeld

## Referencias

- Docs, M. W. (s.f.). *Base64*. <https://developer.mozilla.org/en-US/docs/Glossary/Base64>.
- Edgar, T. W., y Manz, D. O. (2017). Chapter 2 - science and cyber security. En T. W. Edgar y D. O. Manz (Eds.), *Research methods for cyber security* (p. 33-62). Syngress. doi: <https://doi.org/10.1016/B978-0-12-805349-2.00002-9>
- Sheppard, M., y Carter, M. (1993). In other journals. *IALLT Journal of Language Learning Technologies*, 26(1), 65–66.
- Stallings, W., Brown, L., Bauer, M. D., y Bhattacharjee, A. K. (2012). *Computer security: principles and practice*. Pearson Education Upper Saddle River, NJ, USA.
- Wagner, L. (2020, Nov). *What is entropy in cryptography?* <https://medium.com/qvault/what-is-entropy-in-cryptography-76e1afe0f87a>.