*Los siguientes ejercicios deberán ser resueltos de manera grupal mediante el uso de la herramienta de comunicación COLLAB (http://chat.fce.unse.edu.ar/chat/web/), dialogando y consensuando opiniones con los demás integrantes. Los grupos ya fueron habilitados en la herramienta, para acceder utilice su usuario y contraseña.*

**1- Elija un texto que contenga al menos 200 caracteres, quítele los espacios y signos de puntuación, y proceda a aplicar los métodos de encriptado por substitución monoalfabética que se indican a continuación. Muestre el mensaje original y, en todos los casos, alfabeto de origen, alfabeto de encriptado y criptograma resultante.**

Texto Seleccionado: lamayornovedaddelosemailsdinamicosesquepermitiraninteractuardirectamenteconelmensajerecibidocomoporejemploconfirmarlaasistenciaauneventollenaruncuestionarioexploraruncatalogodeproductosoreservarunahabitaciondehotel

1. **Método César** (desplazamiento = 3)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alfabeto Origen | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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 |
| Alfabeto Encriptado | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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 |

Criptograma resultante

ñdodbrupryhgdgghñrvhodlñuglpdolfrvhvtxhshuolwludplpwhudfwxdugluhfwdohpwhfrqhñohpvdmhuhflelgrfrprsruhmhpsirfrpiluoduñddvlvwhpflddxphyhpwrññhpduxpfxhvwlrpdulrhasñruduxpfdwdñrjrghsurgxfwrsruhvhuyduxpdkdelwdflrpghkrwhñ

1. **Método César generalizado, con un desplazamiento igual a 9**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alfabeto Origen | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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 |
| Alfabeto Encriptado | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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 |

Criptograma resultante

tjujhxavxenmjmmntxbnujqtbmqvjuqlxbnbzdnynauqcqajvqvcnajlcdjamqanlcjunvcnlxvntunvbjrnanlqkqmxlxuxyxanrnuytxlxvñqaujatjjbqbcnlqjjdvnenvcxttnvjadvldnbcqxvjaqxngytxajadvljcjtxoxmnyaxmdlcxbxanbnaejadvjpjkqcjlqxvmnpxcnt

**c) Método ordenado por clave, con clave igual a LICENCIATURA**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alfabeto Origen | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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 |
| Alfabeto Encriptado | | | | | | | | | | | | | | | | | | | | | | | | | | |
| L | I | C | E | N | A | T | U | R | B | D | F | G | H | J | K | M | Ñ | O | P | Q | S | V | W | X | Y | Z |

Criptograma resultante

FLGLYKOHKVNELEENFKPNGLRFPERHLGRCKPNPÑSNMNOGRQROLHRHQNOLCQSLOERONCQLGNHQNCKHNFGNHPLBNONCRIREKCKGKMKONBNGMFKCKHAROGLOFLLPRPQNHCRLLSHNVNHQKFFNHLOSHCSNPQRKHLORKNXMFKOLOSHCLQLFKTKENMOKESCQKPONPNOVLOSHLULIRQLCRKHENUKQNF

1. **Método matricial simple, 5 filas x 6 columnas**

Criptograma resultante

**e) Método matricial ordenado por clave, con clave igual a INGENIERIA**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **I** | **N** | **G** | **E** | **R** | **A** |
| 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 |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alfabeto Origen | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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 |
| Alfabeto Encriptado | | | | | | | | | | | | | | | | | | | | | | | | | | |
| F | L | Q | W | A | G | M | R | X | B | H | N | S | Y | C | I | Ñ | T | Z | D | J | O | U | E | K | P | V |

Criptograma resultante

nfsfpizyiuawfwfwanidasfxndwxyfsxqidadtoañazsxjxzfyxyjazfqjofzwxzaqjfsayjaqiyansaydfbazaqxlxwiqisiñizabasñniqiygxzsfznffdxdjayqxffoyauayjinnayfzoyqoadjxiyfzxiakñnizfzoyqfjfnimiwañziwoqjidizadazufzoyfrflxjfqziywarijan

2 - **Elija un texto que contenga al menos 200 caracteres, quítele los espacios y signos de puntuación, y proceda a aplicar los métodos de encriptado por substitución polialfabética que se indican a continuación. Muestre el mensaje original y, en todos los casos, alfabeto de origen, alfabetos de encriptado y criptograma resultante.**

1. **Método de Vigenere, con clave MARZO**

Texto Seleccionado: lamayornovedaddelosemailsdinamicosesquepermitiraninteractuardirectamenteconelmensajerecibidocomoporejemploconfirmarlaasistenciaauneventollenaruncuestionarioexploraruncatalogodeproductosoreservarunahabitaciondehotel

Clave: MARZO

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| l | a | m | a | y | o | r | n | o | v | e | d | a | d | d | e | l | o | s | e | m | a | i | l | s | d | i | n | a | m | i | c | o | s | e | s | q | u | e | p | e | r | m | i | t | i | r | a | n | i | n | t | e |
| M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R |
| r | a | c | t | u | a | r | d | i | r | e | c | t | a | m | e | n | t | e | c | o | n | e | l | m | e | n | s | a | j | e | r | e | c | i | b | i | d | o | c | o | m | o | p | o | r | e | j | e | m | p | l | o |
| Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M |
| c | o | n | f | i | r | m | a | r | l | a | a | s | i | s | t | e | n | c | i | a | a | u | n | e | v | e | n | t | o | l | l | e | n | a | r | u | n | c | u | e | s | t | i | o | n | a | r | i | o | o | e | x |
| A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z |
| p | l | o | r | a | r | u | n | c | a | t | a | l | o | g | o | d | e | p | r | o | d | u | c | t | o | s | r | e | s | e | r | v | a | r | u | n | a | h | a | b | i | t | a | c | i | o | n | d | e | h | o | t |
| O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A | R | Z | O | M | A |
| e | l |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| R | Z |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ENTRADA TEXTO PLANO | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ENTRADA CLAVE |  | 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 |
| A | 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 |
| B | 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 |
| C | 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 |
| D | 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 |
| E | 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 |
| F | 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 |
| G | 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 |
| H | 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 |
| I | 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 |
| J | 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 |
| K | 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 |
| L | 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 |
| M | 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 |
| N | 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 |
| Ñ | 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 |
| O | 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 |
| P | 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 |
| Q | 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 |
| R | 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 |
| S | 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 |
| T | 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 |
| U | 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 |
| V | 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 |
| W | 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 |
| X | 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 |
| Y | 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 |
| Z | 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 |

WADZNAREÑKPDRCRPLGRSXAZKHOIEZATCGRSEQMDEPRDHITRRNWYTWQONTMZGOIJDQFADDQFETNBPLDDBEAADGPCZAWOOTNAAPGQSUEDOZACGMTTRDZGWARRWETVMQTARTBPVVMIALCDBMRMMQGEKSWANRQWAOVWEWOJZGGNTZIMLGFDOEHQDERVRSDVRQJYAYZPTTRBWANUDVATVK

**b) Método periódico, con 3 alfabetos de encriptado elegidos por Ud (pueden ser cualquiera de los métodos de substitución monoalfabética enunciado en el ejercicio anterior).**

5- Tenga en cuenta que es Ud. un espía que ha interceptado cierto mensaje cuya lectura no tiene sentido  
por lo que Ud. supone que está encriptado con algún método de encriptación. Se le pide que intente  
descubrir el texto original del mismo:

“ROTCTILCIGUFUIAAI

EBROEUEIOREUATLDO

TLARRDMONEDNCEION

OERTAAANSSACICDEC

MMLAEDNAOOEIOOANO

EAAPNEOIBDSONNDCN

NDCN no va, si lo incorporamos la mitad del significado del mensaje no tiene sentido

MDROTSSNREDNNODOO

OEURREPFELEDOCEMT

SETCELROEACESEUPR

ENAADPORLBIEPRNAO

LCMRORPMPURVELERS

POARSOOARSSARASAX

RNSECBRCOQULMCTCX”.

Total de caracteres: 225

Caracteres que más veces se repiten

PORCENTAJE = NUM \* 100 / CANTIDAD

E = 23 = 12,4% comparando con la tabla de frecuencias por letras: 16,78%

A = 22 = 9,78% comparando con la tabla de frecuencias por letras: 11,96%

O = 28 = 12,4% comparando con la tabla de frecuencias por letras: 8,69%

L = 10 = 4,4% comparando con la tabla de frecuencias por letras: 8,37%

S = 13 = 5,7% comparando con la tabla de frecuencias por letras: 7,88%

N = 18 = 8% comparando con la tabla de frecuencias por letras: 7,01%

D = 13 = 5,7% comparando con la tabla de frecuencias por letras: 6,87%

Caracteres que medianamente se repiten

R = 23 = 10,2% comparando con la tabla de frecuencias por letras: 4,94%

U = 8 = 3,56% comparando con la tabla de frecuencias por letras: 4,80%

I = 10 = 4,4% comparando con la tabla de frecuencias por letras: 4,15%

T = 9 = 4% comparando con la tabla de frecuencias por letras: 3,31%

C = 16 = 7,11% comparando con la tabla de frecuencias por letras: 2,92%

P = 8 = 3,56% comparando con la tabla de frecuencias por letras: 2,76%

M = 8 = 3,56% comparando con la tabla de frecuencias por letras: 2,12%

Caracteres que pocas veces se repiten

Y = 0 = 0% comparando con la tabla de frecuencias por letras: 1,54%

Q = 1 = 0,4% comparando con la tabla de frecuencias por letras: 1,53%

B = 4 = 1,77% comparando con la tabla de frecuencias por letras: 0,92%

H = 0 = 0% comparando con la tabla de frecuencias por letras: 0,89%

El resto de las letras

G = 1 = 0,4%

F = 2 = 0,8%

Todas las letras tienen frecuencias inferiores a 0,5%

V = 1 = 0,4%

X = 2 = 0,8%

Se puede concluir que no hay mucho margen de error y que las letras del mensaje encriptado pueden conservar su valor, por otro lado, el mensaje no contiene demasiadas letras poco usuales por lo que el método a emplear sería una transposición.

Mensaje original: “RETOMEMOS ELPROBLEMA DE ENCONTRAR LA RUTA MAS CORTA POR CARRETERA ENTRE DOS CIUDADES EL PROBLEMA NOS PROPORCIONA INFORMACION SOBRE EL PROGRESODE LA BUSQUEDA ES DECIR SU FUNCION NOS PERMITE CONOCER LA CALIDAD DE UN ESTADO EN COMPARACION CON OTROS”

Matriz de 17 filas x 13 columnas

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **R** | **E** | **T** | **O** | **M** | **E** | **M** | **O** | **S** | **E** | **L** | **P** | **R** |
| **O** | **B** | **L** | **E** | **M** | **A** | **D** | **E** | **E** | **N** | **C** | **O** | **N** |
| **T** | **R** | **A** | **R** | **L** | **A** | **R** | **U** | **T** | **A** | **M** | **A** | **S** |
| **C** | **O** | **R** | **T** | **A** | **P** | **O** | **R** | **C** | **A** | **R** | **R** | **E** |
| **T** | **E** | **R** | **A** | **E** | **N** | **T** | **R** | **E** | **D** | **O** | **S** | **C** |
| **I** | **U** | **D** | **A** | **D** | **E** | **S** | **E** | **L** | **P** | **R** | **O** | **B** |
| **L** | **E** | **M** | **A** | **N** | **O** | **S** | **P** | **R** | **O** | **P** | **O** | **R** |
| **C** | **I** | **O** | **N** | **A** | **I** | **N** | **F** | **O** | **R** | **M** | **A** | **C** |
| **I** | **O** | **N** | **S** | **O** | **B** | **R** | **E** | **E** | **L** | **P** | **R** | **O** |
| **G** | **R** | **E** | **S** | **O** | **D** | **E** | **L** | **A** | **B** | **U** | **S** | **Q** |
| **U** | **E** | **D** | **A** | **E** | **S** | **D** | **E** | **C** | **I** | **R** | **S** | **U** |
| **F** | **U** | **N** | **C** | **I** | **O** | **N** | **D** | **E** | **E** | **V** | **A** | **L** |
| **U** | **A** | **C** | **I** | **O** | **N** | **N** | **O** | **S** | **P** | **E** | **R** | **M** |
| **I** | **T** | **E** | **C** | **O** | **N** | **O** | **C** | **E** | **R** | **L** | **A** | **C** |
| **A** | **L** | **I** | **D** | **A** | **D** | **D** | **E** | **U** | **N** | **E** | **S** | **T** |
| **A** | **D** | **O** | **E** | **N** | **C** | **O** | **M** | **P** | **A** | **R** | **A** | **C** |
| **I** | **O** | **N** | **C** | **O** | **N** | **O** | **T** | **R** | **O** | **S** | **X** | **X** |