Universidad Nacional Autónoma De México
Facultad De Ciencias

Criptografía y Seguridad

Tarea Examen 1

Fecha:

5 de Noviembre del 2020

Nombre:

Muñiz Patiño, Andrea Fernanda.
Martínez, Alan Alexis
Carmona Mendoza, Martín.

1 Ejercicio 1

a. Sean Z_n y a,b $\in Z_n$ mostrar que : (-a)b = -ab mod (n).

Como sabemos que a,b $\in Z_n$ sabemos que (-a)b $\cong$ -ab mod (n). Pero esto lo podemos ver como (-a)b = nr + -(ab) para alguna -(a,b) perteneciente a Z entonces tenemos que (-a)b = -ab mod (n).

b. Si a $\in Z_n^*$ y ax $\cong$ b mod (n) implica que x $\cong$ ba $_{-1}$ mod (n)

Sabemos que ax $\cong$ b mod (n) lo podemos ver como ax = nr + b para alguna r $\in$ Z entonces como también sabemos que nuestro sistema solo tiene solución si (a,n)= 1 entonces sabemos que a tiene un inverso multiplicativo modulo n entonces si aplicamos ese inverso en ambos lados de la igualdad tenemos que a*a^{-1}*x = n*r¨* a^{-1} + b * a^{-1}.

Pero esto es igual a 1*x = n*r¨* a^{-1} + b * a^{-1}. Como n¨* a^{-1} no afecta mi modulo ya que simplemente lo multiplica quedando el modulo original como en el caso de r $\in$ Z entonces por propiedad esto queda igual x = n *r + b * a^{-1} pero esto es igual a x $\cong$ ba $_{-1}$ mod (n).

c. Si a $\cong$ b mod (n) entonces $a^n \cong b^n$ mod (n)

Sabemos por el pequeño teorema de Fermat que:

Si p es un número primo, o un coprimo con a entonces, para cada número natural a, con a ¿ 0 , ;$a^{p]} \cong$ a (mod p).

Entonces si a $\cong$ b mod (n) sabemos que a $\cong$ a mod (n) entonces:

Si tenemos que (a,n) = 1 por lo que son coprimos entonces tenemos que $a^n \cong$ a mod n .

Análogamente como tenemos la propiedad de que si a $\cong$ b mod (n) entonces b $\cong$ a mod (n) y eso implica que b $\cong$ b mod (n) entonces sabemos que si (b,n) = 1 y por lo que son coprimos entonces tenemos que $b^n \cong$ b mod n .

De lo que podemos concluir que a $\cong$ b mod (n) entonces $a^n \cong b^n$ mod (n) ya que si a $\cong$ b mod (n) y b $\cong b^2$ mod (n) entonces a $\cong b^2$ mod (n) analogamente para a.

2 Ejercicio 2

a. Resolver paso a paso la siguiente congruencia

8x $\cong$ 2 mod (26)

Primero veamos si la congruencia tiene solución entonces saquemos el máximo común divisor (8,26) = 2 y como dos divide a nuestro residuo en este caso a dos entonces podemos concluir que tiene solución.

Entonces pongamos la congruencia en su forma más simple como el residuo es dos podemos divirlo en 2 para tener entonces:

4x $\cong$ 1 mod 13 entonces encontremos el inverso de x mod 13. Podemos notar a simple vista como que como nuestros numeros son muy pequeños que 13 x3 = 39 y por otro lado 4 x 10 es igual a 40 entonces nuestro inverso sería 10 dandonos;

x $\cong$ 10 mod 13 por lo que $\mathbf{x = 13q + 10}$ para alguna q $\in$ Z.

Entonces encontremos el inverso de 8 modulo 26

b. Resolver el siguiente sistema de congruencias de ser posible de lo contrario de una razón especifica de porque no se puede resolver.

x ≅ 4 mod (11)
x ≅ 25 mod (35)
x ≅ 15 mod (22)
x ≅ 5 mod (10)

Verifiquemos si tiene solución lo cuál ocurre solamente sí solo sí (m,n) | (a-b) es decir el máximo común divisor de los módulos divide a la resta de sus residuos.

- (11,35) = 1 entonces 1|(4-25) esto sí se cumple porque en efecto 1|(-21) entonces vamos con el siguiente.
- (11,22) = 11 entonces 11|(4-15) esto sí se cumple porque en efecto 11 | (-11) entonces vamos con el siguiente.
- (11,10) = 1 entonces 1|(4-5) esto sí se cumple porque en efecto 1 | (-1) entonces vamos con el siguiente.
- (35,22) = 1 entonces 1|(25-15) esto sí se cumple porque en efecto 1 | (10) entonces vamos con el siguiente.
- (35,10) = 5 entonces 5|(25-5) esto sí se cumple porque en efecto 5 | (20) entonces vamos con el siguiente.
- (22,10) = 2 entonces 11|(15-5) esto sí se cumple porque en efecto 2 | (20) .

Como podemos observar todos nuestras ecuaciones de nuestro sistema de congruencias cumplen que (m,n) | (a-b) por lo que si tiene solución

Primero nombremos todos nuestras congruencias:

1. x ≅ 4 mod (11)
2. x ≅ 25 mod (35)
3. x ≅ 15 mod (22)
4. x ≅ 5 mod (10)

Entonces tomemos 1.) y veamoslo como una igualdad tal que

5. x = 11r + 4 para alguna r ∈ Z. Y sustituimos en 2.) quedando:

   11r + 4 ≅ 25 mod (35) entonces tenemos que 11r ≅ 25 - 4 mod (35) entonces tenemos:

6. 11r ≅ 21 mod (35) encontramos su inverso como son números pequeños podemos ver que 35 x 5 = 175 y que 11 x 16 = 176 por lo tanto 16 es el inverso de 11 mod 35 entonces tenemos que:

   r ≅ 336 mod (35) = r ≅ 21 mod (35) entonces tenemos .

7. r = 35s + 21 para alguna s ∈ Z y sustituimos en 5 tal que x = 11(35s + 21) + 4 entonces x = 385s + 231 +4 =

8. x = 385s + 235

   Seguimos sustituyendo ahora 3.) en 385s + 235 ≅ 15 mod 22 = 385s ≅ 15 - 235 mod 22 = 385s ≅ -220 mod 22 = 385s ≅ 0 mod 22

9. 385s ≅ 0 mod 22 que podemos verlo como 35s ≅0 mod 2 ya que ambos tiene 11 como factor común. Y como el mod es 2 tenemos que ya es inverso entonces s ≅ 0 mod 2. Por lo tanto s = 2v + 0 para alguna v ∈ Z. Y sustituimos en 8.)

   Quedando 385(2v+0)+235 =

10. x = 770v+235 y sustituimos en 4 quedado:

    770v +235 ≅ 5 mod 10 entonces 770 ≅ -230 mod 10 entonces tenemos que 770 ≅ 0 mod 10 por lo que tenemos 77 ≅ 0 mod 1 pero el inverso multiplicativo es 0 entonces queda 0 ≅ 0 mod 10 por lo que al sustituri en 8. tenemos que x = 385(0) + 235 por lo que queda que **X = 235** como una solución particular.

c. Resolver el siguiente sistema de congruencias de ser posible de lo contrario de una razón especifica de porque no se puede resolver.

   x ≅ 4 mod (7)
   x ≅ 5 mod (33)
   x ≅ 6 mod (14)
   x ≅ 10 mod (22)

   Verifiquemos si tiene solución lo cuál ocurre solamente sí solo sí (m,n) — (a-b) es decir el máximo común divisor de los módulos divide a la resta de sus residuos.

   Entones tenemos:

- (7,33) = 1 entonces 1 | (4-5) esto se cumple ya que 1 —1 entonces pasa.
- (7,14) = 7 entonces 7 | (4-6) esto como vemos no se cumple ya que 7 no divide a -2 entonces como sabemos para que el sistema de congruencias tenga solución necesitamos que se cumpla que (m,n)—(a-b) pero no es este caso no se cumple podemos concluir que el sistema de ecuaciones no tienes solución.

3 Ejercicio 3

a. Sea φ (x) la función de Euler mostrar que φ (p^n) = (p^n) - (p^{n-1})
   Sabemos por le teorema de euler que si (a,m) = 1 entonces $a^{m-1} \cong 1$ mod m o bien que $a^{\varphi(n)} \cong 1$ (mod n).

   Entonces podemos ver a m como m = p_1^{n1} * m = p_2^{n2} * ... * p_r^{nr} y podemos aplicar la función φ de ambos lados quedándonos:

   = $\varphi(m) = \varphi(p_1^{n1} * p_2^{n2} * ... * p_r^{nr})$ pero al ser asociativa la φ de euler tenemos que :

   = $\varphi(m) = \varphi(p_1^{n1}) * (p_2^{n2} * ... * p_r^{nr})$:

   = $\varphi(m) = \varphi(p_1^{n1}) * ((p_2^{n2}) * ... * p_r^{nr})$:

.
.
.
.

$=\varphi(m) = \varphi(p_1^{n1})$ *(p_2^{n2})*...*(p_r^{nr}):

Y como tenemos que si (a,p^n) = 1 si y solo si p no divide a a entonces podemos poner a $\varphi(p^{\ n}) = p^n$ - p^n/ p por lo que podemos concluir que:

$\varphi\ (p^n) = (p^n)$ - (p^{n-1})

b. Dar la cardinalidad de $Z^*_{\ 129}$ y dar sus elementos listados de la forma (a, a1).

(1,1),(2,65),(4,97),(5,26),(7,37),(10,13),(11,47),(13,10),(14,83),(16,121),(17,38),(19,34),(20,71),(22,88),(23,101),(25,31),(26,5),(28,106),(29,89),(31,25),(32,125),(34,19),(37,7),(38,17),(40,100),(41,107),(44,44),(46,115),(47,11),(49,79),(50,80),(52,67),(53,56),(55,61),(56,53),(58,109),(59,129),(61,55),(62,77),(64,127),(65,2),(67,52),(68,74),(70,94),(71,20),(73,76),(74,68),(76,73),(77,62),(79,49),(80,50),(82,118),(83,14),(85,85),(88,22),(89,29),(91,112),(92,122),(94,70),(95,110),(97,4),(98,104),(100,40), (101,23),(103,124),(104,98),(106,28),(107,41),(109,58),(110,95),(112,91),(113,8),(115,46),(116,119),(118,82),(119,116),(121,16),(122,92),(124,103),(125,32),(127,64),(128,1289).

Ejercicio 4

Para el texto proporcionado tenemos dos opciones, o es un texto en español sin ñ, o es un texto en ingles.

Desarrollaremos la idea de que es un texto en español sin **ñ**, ya que al momento de obtener la frecuencia de todas las letras podemos apreciar que solo se contabilizaron 24 letras del texto, por lo cual apoya la idea de que la **ñ** no aparece, y por el número de letras no aparece alguna otra letra del abecedario.

M	153
K	231
B	38
H	67
P	299
I	148
0	267
J	243
T	110
Q	101
G	109
S	152
L	61
D	228
A	20
U	105
C	5
V	13
R	14
X	4
N	10
Z	2
Y	5
E	3

Table 1: Tabla de frecuencias

No aparecen las letras F y W.

Teniendo la tabla de frecuencias de las letra y teniendo el siguiente análisis de las palabras de longitud 1 y dos. Además con el hecho de que estamos trabajando con un codificado en mono-alfabético, sabemos que tendremos un mapeo de letra a letra.

Palabras en el texto cifrado de longitud 1:

- P
- K
- Y
- O

En español tenemos los conectores de **y**, **o**, **a**.
Veamos las repeticiones que tienen esas cuatro letras en nuestro texto cifrado.

M	153
K	231
B	38
H	67
P	299
I	148
0	267
J	243
T	110
Q	101
G	109
S	152
L	61
D	228
A	20
U	105
C	5
V	13
R	14
X	4
N	10
Z	2
Y	5
E	3

Con esto proponemos que $\mathbf{O} = \mathbf{e}$, tomamos esta sustitución ya que si hacíamos el remplazo de $\mathbf{P} = \mathbf{e}$, al tener tantas P's, solas, nos quedarían muchas e como conector en el texto lo cual es poco común, al ser la **O** la siguiente letra que más se repite, al hacer el cambio en el texto obtenemos lo siguiente:

MKBHP IeJTQPG GPS LQDJIDLPGeS AUJIDKJeS MeG MJP Se QeSUHeJ eJ eG GGPHPMK MKBHP IeJTQPG Me GP BeJeTDIP HKGeIUGPQ. **eG** MJP SeHLeJP TPJTK UJP AUJIDKJ PUTKIPTPGDTDIP IKHK UJP AUJIDKJ CeTeQKIPTPGDTDIP TQPJSIQDLIDKJ eJ QJP GP TQP- MUIIDKJ P LQKTeDJPS Se GGeVP P IPRK IKJ HKGMeS K LPTQKJeS Me QJPH, JUJIP IKJ GKS HKGMeS K LPTQKJeS Me MJP. GKS BeJeS GGeBPJ P eXLQeSPQSe AeJKTDLDIPHe- JTe MeRDMK P SU IPLPIDMPM LPQP eSLeIDADIPQ GPS eSTQUITUQPS Me GPS LQKTeDJPS RDKGKBDIPHeJTe PITDVPS. IKMDBK BeJeTDIK GPS QePIIDKJeS RDKNUDHDIPS SKJ HeMDMPS LKQ eJZDHPS, GPS IUP- GeS SKJ TKMPS LQKTeDJPS. GPS LQKTeDJPS SKJ LKGDHeQKS Se SURUJDMPMMeS HKJKHe- QKS MeJKHDJPMKS PHDJKPIDMKS, P HeJUMK GGPHPMKS QeSDMUKS. IPMP PHDJKPIDMK 1TDeJe UJ BQULK PHDJK JCSURDJMDIeMKS eJ UJK Me SUS eXTQeHKS Y UJ BQULK IPQRKXDGK IKKC eJ eG KTQK. JKQHPGHeJTe, Se LUeMeJ eJIKJTQPQ VeDJTe MDAeQeJTeS TDLKS Me PHDJKPIDMKS, eJ UJP SeIUeJIDP eSLeIDADIPHeJTe KQMeJPMP. eJ GP SeIUeJIDP Me JUIGeKTDMKS MeG MJP Se IKMDADIP GP IGPVe JeBPTDVK LPQP GP LQKMUIIDKJ Me LQKTeDJPS. PG JUHeQK Me JUIGeKTDMKS NUe LPQP UJ SKGK PHDJKPIDMK Se Ge Me- JKHDJP IKMKJ. CPY VeDJTe PHDJKPIDMKS IKHUJeS, LeQK

SKGK IUPTQK JUIGeKTDMKS MDAeQeJTeS. KRVDPHeJTe, UJ SDHLGe IKMKJ UJ JUIGeKTDMK NUe IKMDADIP LPQP UJ PHDJKPIDMK LUeMe IKMDADIPQ SKGK LPQP IUPTQK PHDJKPIDMKS. UJ MKRGe IKMDBK MKS JUIGeKTDMKS NUe IKMDADIPJ LPQP UJ PHDJKPIDMK LeQHDTe SKGK MDeIDSeDS IKHRDJPIDKJeS. LKQ GK TPJTK Y MeSMe eG LUJTK Me VDSTP HPTeHPTDIK, UJ TQDLGe IKMDBK TQeS JUIGeKTDMKS NUe IKMDADIPJ LPQP UJ PHDJKPIDMK eS GP UJDMPM Me IKMDADIPIDKJ HPS LeNUeJP IKMKJ IPLPZ Me PEUSTPQSe P GKS VeDJTe PHDJKPIDMKS. GP eVDMeJIDP eXLeQDHeJTPG NUe PLKYP eG IKJIeLTK MeG TQDLGe IKMDBK AUe LQK- LKQIDKJPMP LKQ eG eSTUMDK Me GP PMDIDKJ Me UJ SKGK LPQ Me RPSeS SeJIDGGPS PG BQULK Me eJGPIe SeJIDGGK Me UJ RPITeQDKBQPAK. SD GP TQPJSIQDLIDKJ Me UJP UJDMPM BeJeTDIP AUJIDKJPG IDSTQKJ Me MJP eJ QJPH SDeHLQe Se Gee MeSMe UJP LKSDIDKJ ADEP, eJTKJIeS GKS LQDHeQKS SeDS IKMKJeS Me UJP IPMeJP Me UJ IDSTQKJ Me MJP LKMQDP SeQ GP SDBUDeJTe: TDPHDJPIDTKSDJPPMeJDJP BUPJDJPBUPJDJPIDTKSDJP TDPHDJPPMeJDJPPMeDJP PMeD- JPBUPJDJPTDPHDJP IDTKSDJPBUPJDJPBUPJDJP TDPHDJPIDTKSDJPBUPJDJP GP PMDIDKJ Me UJP SKGP RPSe LKQ eEeHLGK BUPJDJP PG ADJPG MeG SeBUJMK IKMKJ LKMQDP MeSVDPQ K PGTeQPQ TKMKS GKS MeHPS IKMKJeS Me UJ JUIGeKTDMK AUQeP MeG QeBDSTQK e DHLeMDQ GP GeITUQP IKQQeITP Me TKMKS GKS IKMKJeS SDTUPMKS P GP MeQeICP Me GP RPSe PJPMDMP. TDPHDJPIDTKSDJPPMeJDJP BUPJDJPBUPJDJPIDTKIDJP BUPJDJPTDPHDJPPMeJDJP PMeD- JPPMeDJPBUPJDJP TDPHDJPIDTKSDJPBUPJDJP BUPJDJPTDPHDJPIDTKSDJP BUPJDJP Me HPJeQP PJPGKBP IKJ GP eGDHDJPIDKJ Me JUIGeKTDMKS. TQeS eGDHDJPIDKJeS K HUGTDLGKS Me TQeS LUeMeJ IKQQeBDQ GP GeITUQP eJ GP SDJTeSDS Me UJP LQKTeDJP PITDVP. KTQPS eVDMeJIDPS DJMDIPJ NUe eG IKMKJ eS UJP SeIUeJIDP Me TQeS HUIGeK- TDMKS Y Me PNUD NUe PG IKMDBK BeJeTDIK Se Ge IKJKIP IKHK UJ TQDLGeTe K UJP TeQIDP.

Ahora la letra a es la que más se repite, entonces hacemos la sustitución de la $\mathbf{P} = \mathbf{a}$ y veamos que obtenemos...

MKBHa IeJTQaG GaS LQDJIDLaGeS AUJIDKJeS MeG MJa Se QeSUHeJ eJ eG GGaHaMK MKBHa IeJTQaG Me **Ga** BeJeTDIa HKGeIUGaQ. **eG** MJa SeHLeJa TaJTK UJa AUJIDKJ aUTKIaTaGDTDIa IKHK UJa AUJIDKJ CeTeQKIaTaGDTDIa TQaJSIQDLIDKJ eJ QJa Ga TQa- MUIIDKJ a LQKTeDJaS Se GGeVa a IaRK IKJ HKGMeS K LaTQKJeS Me QJaH, JUJIa IKJ GKS HKGMeS K LaTQKJeS Me MJa. GKS BeJeS GGeBaJ a eXLQeSaQSe AeJKTDLDIaHe- JTe MeRDMK a SU IaLaIDMaM LaQa eSLeIDADIaQ GaS eSTQUITUQaS Me GaS LQKTeDJaS RDKGKBDIaHeJTe aITDVaS. IKMDBK BeJeTDIK GaS QeaIIDKJeS RDKNUDHDIaS SKJ HeMDMaS LKQ eJZDHaS, GaS IUa- GeS SKJ TKMaS LQKTeDJaS. GaS LQKTeDJaS SKJ LKGDHeQKS Se SURUJDMaMMeS HKJKHe- QKS MeJKHDJaMKS aHDJKaIDMKS, a HeJUMK GGaHaMKS QeSDMUKS. IaMa aHDJKaIDMK 1TDeJe UJ BQULK aHDJK JCSURDJMDIeMKS eJ UJK Me SUS eXTQeHKS Y UJ BQULK IaQRKXDGK IKKC eJ eG KTQK. JKQHaGHeJTe, Se LUeMeJ eJIKJTQaQ VeDJTe MDAeQeJTeS TDLKS Me aHDJKaIDMKS, eJ UJa SeIUeJIDa eSLeIDADIaHeJTe KQMeJaMa. eJ Ga SeIUeJIDa Me JUIGeKTDMKS MeG MJa Se IKMDADIa Ga IGaVe JeBaTDVK LaQa Ga LQKMUIIDKJ Me LQKTeDJaS. aG JUHeQK Me JUIGeKTDMKS NUe LaQa UJ SKGK aHDJKaIDMK Se Ge MeJKHDJa IKMKJ. CaY VeDJTe aHDJKaIDMKS IKHUJeS, LeQK SKGK IUaTQK JUIGeKTDMKS MDAeQeJTeS. KRVDaHeJTe, UJ SDHLGe IKMKJ UJ JUIGeKTDMK NUe IKMDADIa LaQa UJ aHDJKaIDMK LUeMe IKMDADIaQ SKGK LaQa IUaTQK aHDJKaIDMKS. UJ MKRGe IKMDBK MKS JUIGeKTDMKS NUe IKMDADIaJ LaQa UJ aHDJKaIDMK LeQHDTe SKGK MDeIDSeDS IKHRDJaIDKJeS. LKQ GK TaJTK Y MeSMe eG LUJTK Me VDSTa HaTeHaTDIK, UJ TQDLGe IKMDBK TQeS JUIGeKTDMKS NUe IKMDADIaJ LaQa UJ aHDJKaIDMK eS Ga UJDMaM Me IKMDADIaIDKJ HaS LeNUeJa IKMKJ IaLaZ Me aEUSTaQSe a GKS VeDJTe aHDJKaIDMKS. Ga eVDMeJIDa eXLeQDHeJTaG NUe aLKYa eG IKJIeLTK MeG TQDLGe IKMDBK AUe LQK- LKQIDKJaMa LKQ eG eSTUMDK Me Ga aMDIDKJ Me UJ SKGK LaQ Me RaSeS SeJIDGGaS aG BQULK Me eJGaIe SeJIDGGK Me UJ RaITeQDKBQaAK. SD Ga TQaJSIQDLIDKJ Me UJa UJDMaM BeJeTDIa AUJIDKJaG IDSTQKJ Me MJa eJ QJaH SDeHLQe Se Gee MeSMe UJa LKSDIDKJ ADEa, eJTKJIeS GKS LQDHeQKS SeDS IKMKJeS Me UJa IaMeJa Me UJ IDSTQKJ Me MJa LKMQDa SeQ Ga SDBUDeJTe: TDaHDJaIDTKSDJaaMeJDJa BUaJDJaBUaJDJaIDTKSDJa TDaHDJaaMeJDJaaMeDJa aMeD- JaBUaJDJaTDaHDJa IDTKSDJaBUaJDJaBUaJDJa TDaHDJaIDTKSDJaBUaJDJa Ga aMDIDKJ Me UJa SKGa RaSe LKQ eEeHLGK BUaJDJa aG ADJaG MeG SeBUJMK IKMKJ LKMQDa MeSVDaQ K aGTeQaQ TKMKS GKS MeHaS IKMKJeS Me UJ JUIGeKTDMK AUQea MeG QeBDSTQK e DHLeMDQ Ga GeITUQa IKQQeITa Me TKMKS GKS IKMKJeS SDTUaMKS a Ga MeQeICa Me Ga RaSe aJaMDMa. TDaHDJaIDTKSDJaaMeJDJa BUaJDJaBUaJDJaIDTKIDJa BUaJDJaTDaHDJaaMeJDJa

aMeD- JaaMeDJaBUaJDJa TDaHDJaIDTKSDJaBUaJDJa BUaJDJaTDaHDJaIDTKSDJa BUaJDJa Me HaJeQa aJaGKBa IKJ Ga eGDHDJaIDKJ Me JUIGeKTDMKS. TQeS eGDHDJaIDKJeS K HUGTDLGKS Me TQeS LUeMeJ IKQQeBDQ Ga GeITUQa eJ Ga SDJTeSDS Me UJa LQKTeDJa aITDVa. KTQaS eVDMeJIDaS DJMDIaJ NUe eG IKMKJ eS UJa SeIUeJIDa Me TQeS HUIGeK- TDMKS Y Me aNUD NUe aG IKMDBK BeJeTDIK Se Ge IKJKIa IKHK UJ TQDLGeTe K UJa TeQIDa.

Con las palabras de tamaño dos en negritas, podemos suponer que la $\mathbf{G = l}$ para poder formar los artículos **el** y **la**. Realizando la sustituación tenemos lo siguiente:

MKBHa IeJTQal laS LQDJIDLaleS AUJIDKJeS Mel MJa Se QeSUHeJ eJ el llaHaMK MKBHa IeJTQal Me la BeJeTDIa HKleIUlaQ. el MJa SeHLeJa TaJTK UJa AUJIDKJ aUTKIaTalDTDIa IKHK UJa AUJIDKJ CeTeQKIaTalDTDIa TQaJSIQDLIDKJ eJ QJa la TQa- MUIIDKJ a LQKTeDJaS Se lleVa a IaRK IKJ HKlMeS K LaTQKJeS Me QJaH, JUJIa IKJ lKS HKlMeS K LaTQKJeS Me MJa. lKS BeJeS lleBaJ a eXLQeSaQSe AeJKTDLDIaHe- JTe MeRDMK a SU IaLaIDMaM LaQa eSLeIDADIaQ laS eSTQUITUQaS Me laS LQKTeDJaS RDKlKBDIaHeJTe aITDVaS. IKMDBK BeJeTDIK laS QeaIIDKJeS RDKNUDHDIaS SKJ HeMDMaS LKQ eJZDHaS, laS IUa- leS SKJ TKMaS LQKTeDJaS. laS LQKTeDJaS SKJ LKlDHeQKS Se SURUJDMaMMeS HKJKHe- QKS MeJKHDJaMKS aHDJKaIDMKS, a HeJUMK llaHaMKS QeSDMUKS. IaMa aHDJKaIDMK 1TDeJe UJ BQULK aHDJK JCSURDJMDIeMKS eJ UJK Me SUS eXTQeHKS Y UJ BQULK IaQRKXDlK IKKC eJ el KTQK. JKQHalHeJTe, Se LUeMeJ eJIKJTQaQ VeDJTe MDAeQeJTeS TDLKS Me aHDJKaIDMKS, eJ UJa SeIUeJIDa eSLeIDADIaHeJTe KQMeJaMa. eJ la SeIUeJIDa Me JUlleKTDMKS Mel MJa Se IKMDADIa la IlaVe JeBaTDVK LaQa la LQKMUIIDKJ Me LQKTeDJaS. al JUHeQK Me JUlleKTDMKS NUe LaQa UJ SKlK aHDJKaIDMK Se le Me- JKHDJa IKMKJ. CaY VeDJTe aHDJKaIDMKS IKHUJeS, LeQK SKlK IUaTQK JUlleKTDMKS MDAeQeJTeS. KRVDaHeJTe, UJ SDHLle IKMKJ UJ JUlleKTDMK NUe IKMDADIa LaQa UJ aHDJKaIDMK LUeMe IKMDADIaQ SKlK LaQa IUaTQK aHDJKaIDMKS. UJ MKRle IKMDBK MKS JUlleKTDMKS NUe IKMDADIaJ LaQa UJ aHDJKaIDMK LeQHDTe SKlK MDeIDSeDS IKHRDJaIDKJeS. LKQ lK TaJTK Y MeSMe el LUJTK Me VDSTa HaTeHaTDIK, UJ TQDLle IKMDBK TQeS JUlleKTDMKS NUe IKMDADIaJ LaQa UJ aHDJKaIDMK eS la UJDMaM Me IKMDADIaIDKJ HaS LeNUeJa IKMKJ IaLaZ Me aEUSTaQSe a lKS VeDJTe aHDJKaIDMKS. la eVDMeJIDa eXLeQDHeJTal NUe aLKYa el IKJIeLTK Mel TQDLle IKMDBK AUe LQK- LKQIDKJaMa LKQ el eSTUMDK Me la aMDIDKJ Me UJ SKlK LaQ Me RaSeS SeJIDllaS al BQULK Me eJlaIe SeJIDllK Me UJ RaITeQDKBQaAK. SD la TQaJSIQDLIDKJ Me UJa UJDMaM BeJeTDIa AUJIDKJal IDSTQKJ Me MJa eJ QJaH SDeHLQe Se lee MeSMe UJa LKSDIDKJ ADEa, eJTKJIeS lKS LQDHeQKS SeDS IKMKJeS Me UJa IaMeJa Me UJ IDSTQKJ Me MJa LKMQDa SeQ la SDBUDeJTe: TDaHDJaIDTKSDJaaMeJDJa BUaJDJaBUaJDJaIDTKSDJa TDaHDJaaMeJDJaaMeDJa aMeD- JaBUaJDJaTDaHDJa IDTKSDJaBUaJDJaBUaJDJa TDaHDJaIDTKSDJaBUaJDJa la aMDIDKJ Me UJa SKla RaSe LKQ eEeHLlK BUaJDJa al ADJal Mel SeBUJMK IKMKJ LKMQDa MeSVDaQ K alTeQaQ TKMKS lKS MeHaS IKMKJeS Me UJ JUlleKTDMK AUQea Mel QeBDSTQK e DHLeMDQ la leITUQa IKQQeITa Me TKMKS lKS IKMKJeS SDTUaMKS a la MeQeICa Me la RaSe aJaMDMa. TDaHDJaIDTKSDJaaMeJDJa BUaJDJaBUaJDJaIDTKIDJa BUaJDJaTDaHDJaaMeJDJa aMeD- JaaMeDJaBUaJDJa TDaHDJaIDTKSDJaBUaJDJa BUaJDJaTDaHDJaIDTKSDJa BUaJDJa Me HaJeQa aJalKBa IKJ la elDHDJaIDKJ Me JUlleKTDMKS. TQeS elDHDJaIDKJeS K HUlTDLlKS Me TQeS LUeMeJ IKQQeBDQ la leITUQa eJ la SDJTeSDS Me UJa LQKTeDJa aITDVa. KTQaS eVDMeJIDaS DJMDIaJ NUe el IKMKJ eS UJa SeIUeJIDa Me TQeS HUlleK- TDMKS Y Me aNUD NUe al IKMDBK BeJeTDIK Se le IKJKIa IKHK UJ TQDLleTe K UJa TeQIDa.

Por nuestra elección de idioma tenemos la posibilidades
En español palabras de longitud dos tenemos las siguientes: mi, tu, el, la.
Además observemos que las palabras de tamaño 2 que tenemos son:

- PG
- MO
- GP
- OG
- SD
- UJ

- OJ
- SO
- SU

Y con las sustituciones que tenemos hasta ahora obtuvimos que **GP = la, GO = le, PG = al, OG = el, OJ = eJ** , con ello ya tendríamos los articulos **la, le, al, el** formados, con OJ podemos proponer que **J = n** o **J = s**, sin embargo, para **GPS** que obtenemos hasta ahora **laS**, no habría otra opción, más que la **s**, por lo cual haremos dos sustituciones a la vez y evaluaremos que obtenemos, es decir, sustituiremos **J = n y S = s**

MKBHa IenTQal las LQDnIDLales AUnIDKnes **Mel** Mna se QesUHen en el llaHaMK MKBHa IenTQal Me la BeneTDIa HKleIUlaQ. el Mna seHLena TanTK Una AUnIDKn aUTKIaTalDTDIa IKHK Una AUnIDKn CeTeQKIaTalDTDIa TQansIQDLIDKn en Qna la TQaMUIIDKn a LQKTeDnas se lleVa a IaRK IKn HKlMes K LaTQKnes Me QnaH, nUnIa IKn lKs HKlMes K LaTQKnes Me Mna. lKs Benes lleBan a eXLQesaQse AenKTDLDIaHenTe MeRDMK a sU IaLaIDMaM LaQa esLeIDADIaQ las esTQUITUQas Me las LQKTeDnas RDKlKBDIaHenTe aITDVas. IKMDBK BeneTDIK las QeaIIDKnes RDKNUDHDIas sKn HeMDMas LKQ enZDHas, las IUales sKn TKMas LQKTeDnas. las LQKTeDnas sKn LKlDHeQKs se sURUnDMaMMes HKnKHeQKs MenKHDnaMKs aHDnKaIDMKs, a HenUMK llaHaMKs QesDMUKs. IaMa aHDnKaIDMK 1TDene Un BQULK aHDnK nCsURDnMDIeMKs en UnK Me sUs eXTQeHKs Y Un BQULK IaQRKXDlK IKKC en el KTQK. nKQHalHenTe, se LUeMen enIKnTQaQ VeDnTe MDAeQenTes TDLKs Me aHDnKaIDMKs, en Una seIUenIDa esLeIDADIaHenTe KQMenaMa. en la seIUenIDa Me nUlleKTDMKs Mel Mna se IKMDADIa la llaVe neBaTDVK LaQa la LQKMUIIDKn Me LQKTeDnas. al nUHeQK Me nUlleKTDMKs NUe LaQa Un sKlK aHDnKaIDMK se le MenKHDna IKMKn. CaY VeDnTe aHDnKaIDMKs IKHUnes, LeQK sKlK IUaTQK nUlleKTDMKs MDAeQenTes. KRVDaHenTe, Un sDHLle IKMKn Un nUlleKTDMK NUe IKMDADIa LaQa Un aHDnKaIDMK LUeMe IKMDADIaQ sKlK LaQa IUaTQK aHDnKaIDMKs. Un MKRle IKMDBK MKs nUlleKTDMKs NUe IKMDADIan LaQa Un aHDnKaIDMK LeQHDTe sKlK MDeIDseDs IKHRDnaIDKnes. LKQ lK TanTK Y MesMe el LUnTK Me VDsTa HaTeHaTDIK, Un TQDLle IKMDBK TQes nUlleKTDMKs NUe IKMDADIan LaQa Un aHDnKaIDMK es la UnDMaM Me IKMDADIaIDKn Has LeNUena IKMKn IaLaZ Me aEUsTaQse a lKs VeDnTe aHDnKaIDMKs. la eVDMenIDa eXLeQDHenTal NUe aLKYa el IKnIeLTK Mel TQDLle IKMDBK AUe LQKLKQIDKnaMa LKQ el esTUMDK Me la aMDIDKn Me Un sKlK LaQ Me Rases senIDllas al BQULK Me enlaIe senIDllK Me Un RaITeQDKBQaAK. sD la TQansIQDLIDKn Me Una UnDMaM BeneTDIa AUnIDKnal IDsTQKn Me Mna en QnaH sDeHLQe se lee MesMe Una LKsDIDKn ADEa, enTKnIes lKs LQDHeQKs seDs IKMKnes Me Una IaMena Me Un IDsTQKn Me Mna LKMQDa seQ la sDBUDenTe: TDaHDnaIDTKsDnaaMenDna BUanDnaBUanDnaIDTKsDna TDaHDnaaMenDnaaMeDna aMeDnaBUanDnaTDaHDna IDTKsDnaBUanDnaBUanDna TDaHDnaIDTKsDnaBUanDna la aMDIDKn Me Una sKla Rase LKQ eEeHLlK BUanDna al ADnal Mel seBUnMK IKMKn LKMQDa MesVDaQ K alTeQaQ TKMKs lKs MeHas IKMKnes Me Un nUlleKTDMK AUQea Mel QeBDsTQK e DHLeMDQ la leITUQa IKQQeITa Me TKMKs lKs IKMKnes sDTUaMKs a la MeQeICa Me la Rase anaMDMa. TDaHDnaIDTKsDnaaMenDna BUanDnaBUanDnaIDTKIDna BUanDnaTDaHDnaaMenDna aMeDnaaMeDnaBUanDna TDaHDnaIDTKsDnaBUanDna BUanDnaTDaHDnaIDTKsDna BUanDna Me HaneQa analKBa IKn la elDHDnaIDKn Me nUlleKTDMKs. TQes elDHDnaIDKnes K HUlTDLlKs Me TQes LUeMen IKQQeBDQ la leITUQa en la sDnTesDs Me Una LQKTeDna aITDVa. KTQas eVDMenIDas DnMDIan NUe el IKMKn es **Una** seIUenIDa Me TQes HUlleK- TDMKs Y Me aNUD NUe al IKMDBK BeneTDIK se le IKnKIa IKHK Un TQDLleTe K **Una** TeQIDa.

Con esas sustituciones podemos ver en negritas las palabras Mel de tamaño 3 que tenemos en el texto, al principio del texto y al final tenemos en negritas Una. Con lo que podemos hacer las siguientes deducciones: **U = u y M = d**, obteniendo:

dKBHa IenTQal las LQDnIDLales AunIDKnes del dna se QesuHen en el llaHadK dKBHa IenTQal de la BeneTDIa HKleIulaQ. el dna seHLena TanTK una AunIDKn auTKIaTalDTDIa IKHK una AunIDKn CeTeQKIaTalDTDIa TQansIQDLIDKn en Qna la TQaduIIDKn a LQKTeDnas se **lleVa** a IaRK IKn HKldes K LaTQKnes de QnaH, nunIa IKn lKs HKldes K LaTQKnes de dna. lKs Benes lleBan a eXLQesaQse AenKTDLDIaHenTe deRDdK a su IaLaIDdad LaQa esLeIDADIaQ las esTQuITuQas de las LQKTeDnas RDKlKBDIaHenTe aITDVas. IKdDBK BeneTDIK las QeaIIDKnes RDKNuDHDIas sKn HedDdas LKQ enZDHas, las Iuales sKn TKdas LQKTeDnas. las LQKTeDnas sKn LKlDHeQKs se suRunDdaddes HKnKHe- QKs denKHDnadKs

aHDnKaIDdKs, a HenudK llaHadKs QesDduKs. Iada aHDnKaIDdK 1TDene un BQuLK aHDnK nCsuRDndDIedKs en unK de sus eXTQeHKs Y un BQuLK IaQRKXDlK IKKC en el KTQK. nKQHalHenTe, se Lueden enIKnTQaQ VeDnTe dDAeQenTes TDLKs de aHDnKaIDdKs, en una seIuenIDa esLeIDADIaHenTe KQdenada. en la seIuenIDa de nuIleKTDdKs del dna se IKdDADIa la **IlaVe** neBaTDVK LaQa la LQKduIIDKn de LQKTeDnas. al nuHeQK de nuIleKTDdKs Nue LaQa un sKlK aHDnKaIDdK se le denKHDna IKdKn. CaY VeDnTe aHDnKaIDdKs IKHunes, LeQK sKlK IuaTQK nuIleKTDdKs dDAeQenTes. KRVDaHenTe, un sDHLle IKdKn un nuIleKTDdK Nue IKdDADIa LaQa un aHDnKaIDdK Luede IKdDADIaQ sKlK LaQa IuaTQK aHDnKaIDdKs. un dKRle IKdDBK dKs nuIleKTDdKs Nue IKdDADIan LaQa un aHDnKaIDdK LeQHDTe sKlK dDeIDseDs IKHRDnaIDKnes. LKQ lK TanTK Y desde el LunTK de VDsTa HaTeHaTDIK, un TQDLle IKdDBK TQes nuIleKTDdKs Nue IKdDADIan LaQa un aHDnKaIDdK es la unDdad de IKdDADIaIDKn Has LeNuena IKdKn IaLaZ de aEusTaQse a lKs VeDnTe aHDnKaIDdKs. la eVDdenIDa eXLeQDHenTal Nue aLKYa el IKnIeLTK del TQDLle IKdDBK Aue LQKLKQIDKnada LKQ el esTudDK de la adDIDKn de un sKlK LaQ de Rases senIDllas al BQuLK de enlaIe senIDllK de un RaITeQDKBQaAK. sD la TQansIQDLIDKn de una unDdad BeneTDIa AunIDKnal IDsTQKn de dna en QnaH sDeHLQe se lee desde una LKsDIDKn ADEa, enTKnIes lKs LQDHeQKs seDs IKdKnes de una Iadena de un IDsTQKn de dna LKdQDa seQ la sDBuDenTe: TDaHDnaIDTKsDnaadenDna BuanDnaBuanDnaIDTKsDna TDaHDnaadenDnaadeDna adeDnaBuanDnaTDaHDna IDTKsDnaBuanDnaBuanDna TDaHDnaIDTKsDnaBuanDna la adDIDKn de una sKla Rase LKQ eEeHLlK BuanDna al ADnal del seBundK IKdKn LKdQDa desVDaQ K alTeQaQ TKdKs lKs deHas IKdKnes de un nuIleKTDdK AuQea del QeBDsTQK e DHLedDQ la leITuQa IKQQeITa de TKdKs lKs IKdKnes sDTuadKs a la deQeICa de la Rase anadDda. TDaHDnaIDTKsDnaadenDna BuanDnaBuanDnaIDTKIDna BuanDnaTDaHDnaadenDna adeDnaadeDnaBuanDna TDaHDnaIDTKsDnaBuanDna BuanDnaTDaHDnaIDTKsDna BuanDna de HaneQa analKBa IKn la elDHDnaIDKn de nuIleKTDdKs. TQes elDHDnaIDKnes K HulTDLlKs de TQes Lueden IKQQeBDQ la leITuQa en la sDnTesDs de una LQKTeDna aITDVa. KTQas eVDdenIDas DndDIan Nue el IKdKn es una seIuenIDa de TQes HuIleK- TDdKs Y de aNuD Nue al IKdDBK BeneTDIK se le IKnKIa IKHK un TQDLleTe K una TeQIDa.

Con ello obtenemos por ahora la siguiente tabla de correspondencia.

A	B	C	D	E
p			m	o
F	G	H	I	J

K	L	M	N	Ñ
	g		j	
O	P	Q	R	S
				s
T	U	V	W	X
	u			
Y	Z			

Podemos observar que en la letra **s** y **u** coinciden las letras. Por tener esa conincidencia jugamos y hacemos la sustitución de $\mathbf{V} = \mathbf{v}$ y por la palabra resaltada en negritas hacemos la sustitución de $\mathbf{C} = \mathbf{i}$ obteniendo el siguiente texto y la siguiente correspondencia:

dKBHa IenTQal las LQDnIDLales AunIDKnes del dna se QesuHen en el llaHadK dKBHa IenTQal de la BeneTDIa HKleIulaQ. el dna seHLena TanTK una AunIDKn auTKIaTalDTDIa IKHK una AunIDKn ieTeQKIaTalDTDIa TQansIQDLIDKn en Qna la TQaduIIDKn a LQKTeDnas se lleva a IaRK IKn HKldes K LaTQKnes de QnaH, nunIa IKn lKs HKldes K LaTQKnes de dna. lKs Benes lleBan a eXLQesaQse AenKTDLDIaHenTe deRDdK a su IaLaIDdad LaQa esLeIDADIaQ las esTQuITuQas de las LQKTeDnas RDKlKBDIaHenTe aITDvas. IKdDBK BeneTDIK las QeaIIDKnes RDKNuDHDIas sKn HedDdas LKQ enZDHas, las Iuales sKn TKdas LQKTeDnas. las LQKTeDnas sKn LKlDHeQKs se suRunDdaddes HKnKHe- QKs denKHDnadKs aHDnKaIDdKs, a HenudK llaHadKs QesDduKs. Iada aHDnKaIDdK 1TDene un BQuLK aHDnK nisuRDndDIedKs en unK de sus eXTQeHKs Y un BQuLK IaQRKXDlK IKKi en el KTQK. nKQHalHenTe, se Lueden enIKnTQaQ veDnTe dDAeQenTes TDLKs de aHDnKaIDdKs, en una seIuenIDa esLeIDADIaHenTe KQdenada. en la seIuenIDa de nuIleKTDdKs del dna se IKdDADIa la Ilave neBaTDvK LaQa la LQKduIIDKn de LQKT-

eDnas. al nuHeQK de nuIleKTDdKs Nue LaQa un sKlK aHDnKaIDdK se le denKHDna IKdKn. iaY veDnTe aHDnKaIDdKs IKHunes, LeQK sKlK IuaTQK nuIleKTDdKs dDAeQenTes. KRvDaHenTe, un sDHLle IKdKn un nuIleKTDdK Nue IKdDADIa LaQa un aHDnKaIDdK Luede IKdDADIaQ sKlK LaQa IuaTQK aHDnKaIDdKs. un dKRle IKdDBK dKs nuIleKTDdKs Nue IKdDADIan LaQa un aHDnKaIDdK LeQHDTe sKlK dDeIDseDs IKHRDnaIDKnes. LKQ lK TanTK Y desde el LunTK de vDsTa HaTeHaTDIK, un TQDLle IKdDBK TQes nuIleKTDdKs Nue IKdDADIan LaQa un aHDnKaIDdK es la unDdad de IKdDADIaIDKn Has LeNuena IKdKn IaLaZ de aEusTaQse a lKs veDnTe aHDnKaIDdKs. la evDdenIDa eXLeQDHenTal Nue aLKYa el IKnIeLTK del TQDLle IKdDBK Aue LQKLKQIDKnada LKQ el esTudDK de la adDIDKn de un sKlK LaQ de Rases senIDllas al BQuLK de enlaIe senIDllK de un RaITeQDKBQaAK. sD la TQansIQDLIDKn de una unDdad BeneTDIa AunIDKnal IDsTQKn de dna en QnaH sDeHLQe se lee desde una LKsDIDKn ADEa, enTKnIes lKs LQDHeQKs seDs IKdKnes de una Iadena de un IDsTQKn de dna LKdQDa seQ la sDBuDenTe: TDaHDnaIDTKsDnaadenDna BuanDnaBuanDnaIDTKsDna TDaHDnaadenDnaadeDna adeDnaBuanDnaTDaHDna IDTKsDnaBuanDnaBuanDna TDaHDnaIDTKsDnaBuanDna la adDIDKn de una sKla Rase LKQ eEeHLlK BuanDna al ADnal del seBundK IKdKn LKdQDa desvDaQ K alTeQaQ TKdKs lKs deHas IKdKnes de un nuIleKTDdK AuQea del QeBDsTQK e DHLedDQ la leITuQa IKQQeITa de TKdKs lKs IKdKnes sDTuadKs a la deQeIia de la Rase anadDda. TDaHDnaIDTKsDnaadenDna BuanDnaBuanDnaIDTKIDna BuanDnaTDaHDnaadenDna adeDnaadeDnaBuanDna TDaHDnaIDTKsDnaBuanDna BuanDnaTDaHDnaIDTKsDna BuanDna de HaneQa analKBa IKn la elDHDnaIDKn de nuIleKTDdKs. TQes elDHDnaIDKnes K HulTDLlKs de TQes Lueden IKQQeBDQ la leITuQa en la sDnTesDs de una LQKTeDna aITDva. KTQas evDdenIDas DndDIan Nue el IKdKn es una seIuenIDa de TQes HuIleK- TDdKs Y de aNuD Nue al IKdDBK BeneTDIK se le IKnKIa IKHK un TQDLleTe K una TeQIDa.

A	B	C	D	E
p		i	m	o
F	G	H	I	J

K	L	M	N	Ñ
	g		j	
O	P	Q	R	S
				s
T	U	V	W	X
	u	v		
Y	Z			

Con la regla de correspondencia podemos deducir que la palabra clave es **primo** e ir completando la correspondencia con las palabras que faltan. Quedando la correspondencia como se muestra a continuación.

A	B	C	D	E
p	r	i	m	o
F	G	H	I	J
a	b	c	d	e
K	L	M	N	Ñ
f	g	h	j	-
O	P	Q	R	S
k	l	n	q	s
T	U	V	W	X
t	u	v	w	x
Y	Z			
y	z			

Table 2: La Ñ no se considero

Así obtenemos el texto descifrando con esa regla de correspondencia. **NOTA**, para el desarrollo de la tarea

tomó más pasos darnos cuenta de la clave, se simplifica en el presente texto, pero se añade el archivo *Jupyter* donde se estuvieron haciendo las sustituciones para la deducción presentada aquí. En el archivo *Jupyter* se muestra el camino 1 que se hizo para el descubrimiento y el camino 2 que acorto la explicación de la obtención de la llave.

3.1 Texto descifrado

dogma central las principales funciones del dna se resumen en el llamado dogma central de la genetica molecular. el dna sempena tanto una funcion autocatalitica como una funcion heterocatalitica transcripcion en rna la traduccion a proteinas se lleva a cabo con moldes o patrones de rnam, nunca con los moldes o patrones de dna. los genes llegan a expresarse fenotipicamente debido a su capacidad para especificar las estructuras de las proteinas biologicamente activas. codigo genetico las reacciones bioquimicas son medidas por enzimas, las cuales son todas proteinas. las proteinas son polimeros se subunidaddes monome- ros denominados aminoacidos, a menudo llamados residuos. cada aminoacido 1tiene un grupo amino nhsubindicedos en uno de sus extremos y un grupo carboxilo cooh en el otro. normalmente, se pueden encontrar veinte diferentes tipos de aminoacidos, en una secuencia especificamente ordenada. en la secuencia de nucleotidos del dna se codifica la clave negativo para la produccion de proteinas. al numero de nucleotidos que para un solo aminoacido se le denomina codon. hay veinte aminoacidos comunes, pero solo cuatro nucleotidos diferentes. obviamente, un simple codon un nucleotido que codifica para un aminoacido puede codificar solo para cuatro aminoacidos. un doble codigo dos nucleotidos que codifican para un aminoacido permite solo dieciseis combinaciones. por lo tanto y desde el punto de vista matematico, un triple codigo tres nucleotidos que codifican para un aminoacido es la unidad de codificacion mas pequena codon capaz de ajustarse a los veinte aminoacidos. la evidencia experimental que apoya el concepto del triple codigo fue proporcionada por el estudio de la adicion de un solo par de bases sencillas al grupo de enlace sencillo de un bacteriografo. si la transcripcion de una unidad genetica funcional cistron de dna en rnam siempre se lee desde una posicion fija, entonces los primeros seis codones de una cadena de un cistron de dna podria ser la siguiente: tiaminacitosinaadenina guaninaguaninacitosina tiaminaadeninaadeina adeinaguaninatiamina citosinaguaninaguanina tiaminacitosinaguanina la adicion de una sola base por ejemplo guanina al final del segundo codon podria desviar o alterar todos los demas codones de un nucleotido furea del registro e impedir la lectura correcta de todos los codones situados a la derecha de la base anadida. tiaminacitosinaadenina guaninaguaninacitocina guaninatiaminaadenina adeinaadeinaguanina tiaminacitosinaguanina guaninatiaminacitosina guanina de manera analoga con la eliminacion de nucleotidos. tres eliminaciones o multiplos de tres pueden corregir la lectura en la sintesis de una proteina activa. otras evidencias indican que el codon es una secuencia de tres mucleotidos y de aqui que al codigo genetico se le conoca como un triplete o una tercia.

4 Ejercicio 5

Para hacer el descifrado del texto presentado obtuvimos la siguiente tabla:

Secuencia	**Posiciones**	**Distancia**	**Factores**
Z N W C Z	9720, 13844	4,124	
E G A L	5052, 8220	3,168	
Q S W M	1722, 3224	1,502	
Y E M	0, 814,2284,2810, 6440, 10422		
C R R	2910, 9322, 12340, 13434		
N N	1330, 3866, 4916, 11640, 12114		

Con la información obtenida hasta el momento no es posible hacer una suposición, por lo que buscaremos una cadena de al menos longitud cinco que se repita en la secuencia dada.

Secuencia	Posiciones	Distancia	Factores
G C E M Q H V H I	2580, 3722	1,142	$2^* 571$
Z N W C Z	9720, 13844	4,124	$2^2 * 1031$
A F S H R	10302, 11702	1,400	$2^3 * 5^2 * 7$
T O P M F	2664, 5688	3,024	$2 * 3^3 * 7$
E G A L	5052, 8220	3,168	$2 * 3^2 * 11$
Q S W M	1722, 3224	1,502	$2 * 751$
R R N Q	3640, 4690	1,050	$2 * 3 * 5^2 * 7$
R W N A	3602, 5306	1,704	$2^3 * 3 * 71$
Y E M	0, 814,2284,2810, 6440, 10422	814, 1468, 526, 3630 3982	$2 * 11 * 37$ $2 * 2 * 367$ $2 * 263$ $2 * 3 * 5 * 11^2$ $2 * 11 * 181$
C R R	2910, 9322, 12340, 13434	6412, 3018, 1094	$2^2 * 7 * 229$ $2 * 3 * 503$ $2 * 547$
N N	1330, 3866, 4916, 11640, 12114		

Table 3: Tabla de descomposición de factores

El factor común en la tabla es **dos**, sin embargo, sería muy corta, así que nos dimos a la tarea de facilitar el encontrar las subsecuencias y usamos la herramienta que se encuentra en la página http://www.criptored.upm.es/crypt4you/tem

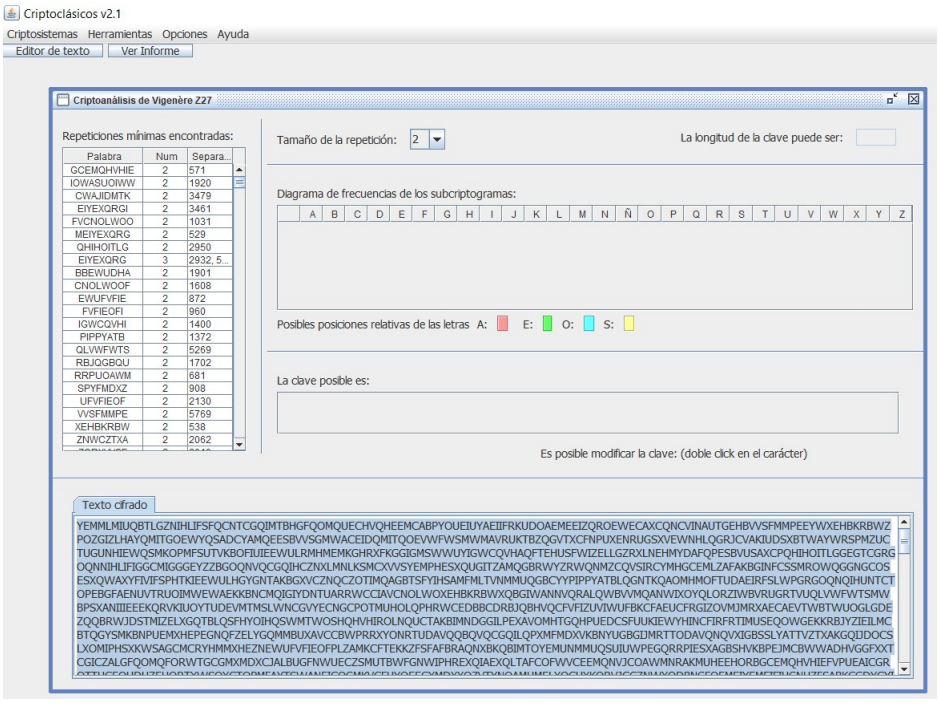


Figure 1: Vista general del programa

El programa se descargo desde la URL: http://www.criptored.upm.es/software/sw$_m$001$c.htmyseinstaloenWindows$.

En el programa Criptoclasicos v2.1 onde se obtuvieron secuencia de mayor tamaño repetidas, no puede descifrarse el texto proporcionado en la tarea, solo puede hacerse un cripto analisis.

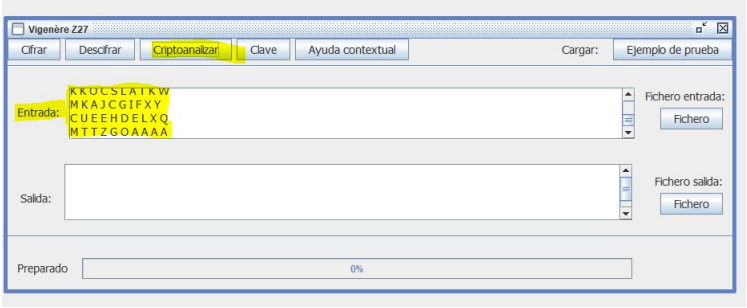


Figure 2: Cripto análisis

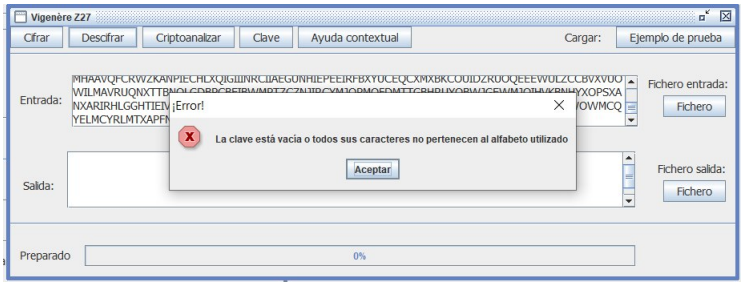


Figure 3: No puede descifrarse

En parte de que no puede descifrarse es por que no hemos obtenido la llave. Y los resultados del cripto-análisis se muestran a continuación:

Palabra	Num	Separa...
GCEMQHVHIE	2	571
IOWASUOIWW	2	1920
CWAJIDMTK	2	3479
EIYEXQRGI	2	3461
FVCNOLWOO	2	1031
MEIYEXQRG	2	529
QHIHOITLG	2	2950
EIYEXQRG	3	2932, 5...
BBEWUDHA	2	1901
CNOLWOOF	2	1608
EWUFVFIE	2	872
FVFIEOFI	2	960
IGWCQVHI	2	1400
PIPPYATB	2	1372
QLVWFWTS	2	5269
RBJQGBQU	2	1702
RRPUOAWM	2	681
SPYFMDXZ	2	908
UFVFIEOF	2	2130
VVSFMMPE	2	5769
XEHBKRBW	2	538
ZNWCZTXA	2	2062

Con los nuevos resultados obtenidos ahora podemos agregar a la tabla 3 nuevos renglones.

Secuencia	Posiciones	Distancia	Factores
G C E M Q H V H I	2580, 3722	1,142	2* 571
Z N W C Z	9720, 13844	4,124	2^2 * 1031
A F S H R	10302, 11702	1,400	2^3 * 5^2 * 7
T O P M F	2664, 5688	3,024	2 * 3^3 * 7
E G A L	5052, 8220	3,168	2 * 3^2 * 11
Q S W M	1722, 3224	1,502	2 * 751
R R N Q	3640, 4690	1,050	2 * 3 * 5^2 * 7
R W N A	3602, 5306	1,704	2^3 * 3 * 71
Y E M	0, 814,2284,2810, 6440, 10422	814, 1468, 526, 3630 3982	2 * 11 * 37 2 * 2 * 367 2 * 263 2 * 3 * 5 * 11^2 2 * 11 * 181
C R R	2910, 9322, 12340, 13434	6412, 3018, 1094	2^2 * 7 * 229 2 * 3 * 503 2 * 547
N N	1330, 3866, 4916, 11640, 12114		
IOWASUOIWW		1920	2 * 3 * 5
CWAJIDMTK		3479	7 * 7 * 71
MEIYEXQRGI		529	23 * 23
QHIHOITLG		2950	2 * 5^2 * 59
EIYEXQRG		2932	2^2 * 733
EWUFVFIE		872	2^3 * 109

Table 4: Resultados obtenidos con la herramienta

La tabla nueva tiene secuencias de tamaño 10 y 9, con solo 2 apariciones las cuales no fueron proporcionadas por la herramienta, pero si la distancia que pudimos descomponer en factores, teniendo ahora las siguientes repeticiones de factores: siete aparece cinco veces, veintidós aparece dos veces, cuatro que puede verse como dos por dos aparece cuatro veces, ocho que aparece por multiplicar tres veces dos aparece dos etc... Sin embargo, el tener una clave de tamaño cuatro o dos es demasiado corta, por lo cual llegamos al acuerdo de hacer la propuesta de que la longitud de la clave es **9** pues aparece dos veces en la tabla 4 y además es MCD de algunas distancias.

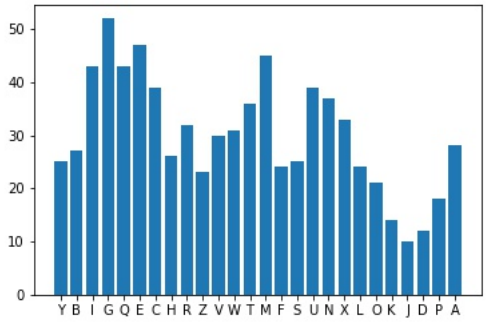
4.1 Frecuencias de letras en cada columna

A continuación se muestran las frecuencias de aparición por columna después de haber separado el texto cifrado en 9 columnas, al inicio el separar el texto en columnas lo hicimos mal y al obtener las frecuencias había datos que no ayudaban para hacer una relación entre la letra que más aparecía en la columna y así asociarla con la **e** que es la letra que más se repite en el idioma Español. La función y resultados pueden visualizarse también en el archivo *jupyter* que acompaña este archivo PDF.

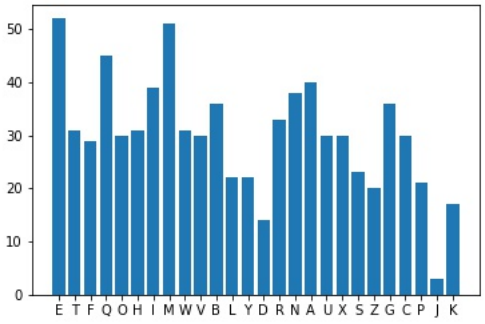
```python
def columnas(x,cadena,col):
    inicio = col - 1
    sig = inicio
    colStri = ""
    while sig < len(cadena):
        #Contatenamos los caracteres de la posición sig
        colStri = colStri + cadena[sig]
        sig = sig + x

    return colStri
```

Figure 4: Función para separar el texto en columnas

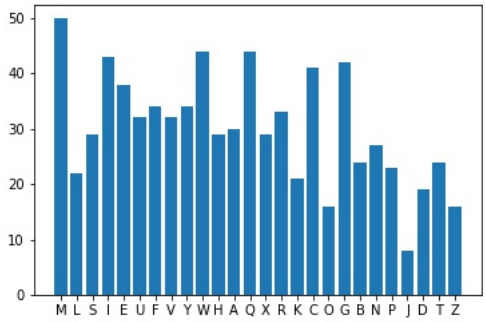
Las gráficas para cada columna se presentan a continuación:



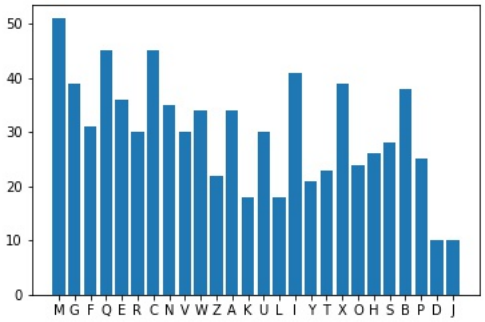
(a) Frecuencias columna 1



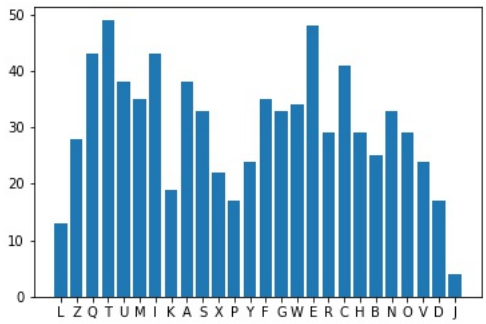
(b) Frecuencias columna 1



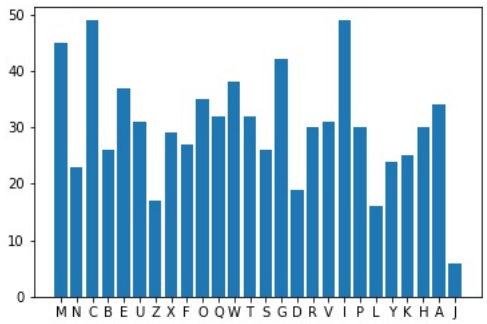
(a) Frecuencias columna 3



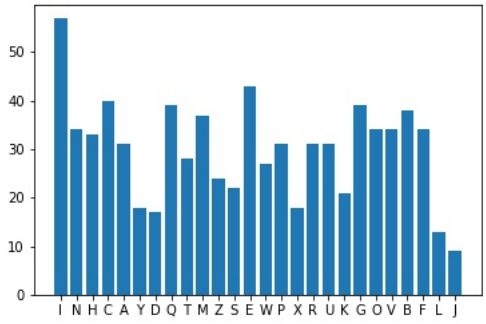
(b) Frecuencias columna 4



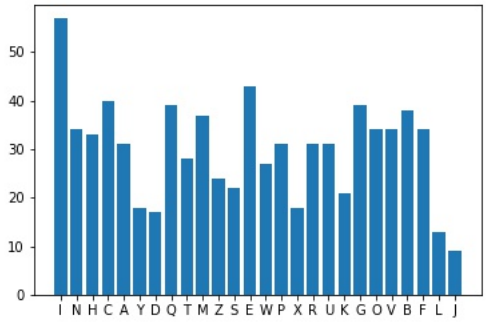
(a) Frecuencias columna 5



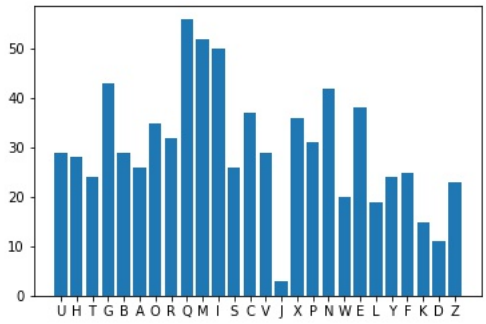
(b) Frecuencias columna 6



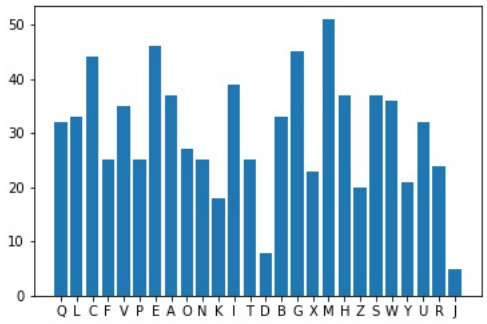
(a) Frecuencias columna 7



(b) Frecuencias columna 7



(a) Frecuencias columna 8



(b) Frecuencias columna 9

4.2 Texto descifrado

Sin embargo para la segunda mitad del texto parece haber un desfase, por lo cual solo sería un desplazamiento de la palabra clave: **NEUMATICO** la cual se obtuvo de obtener las frecuencias de cada columna y relacionarla con la letra más repetida del idioma español, usando además el desplazamiento para ir obteniendo las letras de la palabra clave. Al igual que para el ejercicio 4, en el archivo Jupyter anexo en el classroom están las funciones y calculos para haber llegado a la clave.

Las altas concentraciones de ribo n u c l e o t i d o s en presencia de la enzima p o l i n u c l e o t i d o f o s f o r i l a s a p u e d e n g e n e r a r m o l e c u l a s d e r n a m s i n t e t i c a s i n v i t r o a l f o r m a r u n e n l a c e i n t e r n u c l e o t i d o f o s f o d i e s t e r d e e s t a m a n e r a p u e d e n u n i r s e u n a s c o n o t r a s u n n u m e r o d e m o l e c u l a s d e u r a c i l o y a s i f o r m a r u n a m o l e c u l a s i n t e t i c a d e p o l i u r a c i l o c o

n l a a c t i v i d a d d e r n a m a l a g r e g a r p o l i u r a c i l o a l o s e x t r a c t o s d e c e l u l a s b a c t e r i a n a s s e p r o d u c e u n a s i n t e s i s
l i m i t a d a d e p o l i p e p t i d o s q u e s o l o c o n t i e n e n a l a m i n o a c i d o f e n i l a l a n i n a e s p o r e s t o q u e e s p r o b a b l e q u e s e a
n t r e s u r a c i l o s l o s q u e c o d i f i q u e n p a r a l a s i n t e s i s d e l a f e n i l a l a n i n a l a s m e z c l a s d e d i f e r e n t e s r i b o n u c l e o t i
d o s t a m b i e n p u e d e n f o r m a r m o l e c u l a s s i n t e t i c a s d e r n a m c o n l o s n u c l e o t i d o s d i s p u e s t o s e n u n o r d e n a l a z a r
p u e d e e m p l e a r s e u n a c o m b i n a c i o n d e t e c n i c a s q u i m i c o o r g a n i c a s o e n z i m a t i c a s p a r a l a p r e p a r a c i o n d e p o l i
r r i b o n u c l e o t i d o s s i n t e t i c o s s o n s e c u e n c i a s d e r e p e t i c i o n c o n o c i d a s c o m o p o r e j e m p l o a d e n i n a u r a c i l a d e
n i n a u r a c i l a d e n i n a u r a c i l q u e c o d i f i c a a l t e r n a t i v a m e n t e p a r a l o s a m i n o a c i d o s i s o l e u s i n a y t i r o s i n a c i t o
c i n a u r a c i l c i t o c i n a u r a c i l q u e c o d i f i c a p a r a l a l e u c i n a y s e i n a e n f o r m a a l t e r n a e t c e t e r a i n c l u s o e n a u s e n c i
a d e r n a m y d e s i n t e s i s d e p r o t e i n a s u n t r i n u c l e o t i d o s e f i j a r a a u n r i b o s o m a p o r l o t a n t o i n v i t r o p u e d e n u t i l
i z a r s e t r i n u c l e o t i d o s d e s e c u e n c i a c o n o c i d a p a r a f i j a r s e e s p e c i f i c a m e n t e c o n u n o d e u n a m e z c l a d e v e i n t e
d i f e r e n t e s a m i n o a c i d o s y a s i u n i r s e a l o s r i b o s o m a s p o r e j e m p l o u r a c i l u r a c i l g u a n i n a s o l o f i j a e l r n a t c a r g
a d o d e l e u c i n a a l o s r i b o s o m a s u r a c i l g a u n i n a u r a c i l s o l o f i j a e l r n a t c a r g a d o d e c i s t e i n a e t c e t e r a e l c o d i g o
g e n e t i c o e s d e g e n e r a d o d e b i d o a q u e e x i s t e m a s d e u n c o d o n p a r a l a s i n t e s i s d e l a m a y o r p a r t e d e l o s a m i n o a c i
d o s e l c o d i g o e s b a s i c a m e n t e e l m i s m o p r a t o d o s l o s o r g a n i s m o s a l p a r e c e r d e l o s s e s e n t a y c u a t r o p o s i b l e s c o
d o n e s d e l e t r a s s o l o t r e s s o n i n c a p a c e s d e c o d i f i c a r p a r a c u a l q u i e r a m i n o a c i d o a e s t o s c o d o n e s s e l e s d e n o m
i n a t r i p l e t e s s i n s e n t i d o s i n t e s i s d e p r o t e i n a s l a i n f o r m a c i o n e n u n a s e c u e n c i a d e s o x i r r i b o n u c l e o t i d a e s t
r a n s c r i t a o t r a d u c i d a e n l a s e c u e n c i a r i b o n u c l e o t i d a d e u n a m o l e c u l a d e r n a p o r u n a e n z i m a e s p e c i f i c a r n a
p o l i m e r a s a e n l a d o b l e h e l i c e i n t a c t a e s t a e n z i m a r e c o n o c e c o m o s i t i o d e i n i c i a c i o n c i e r t a s s e c u e n c i a s d e p
a r e s c o n a b u n d a n t e a d e n a i n a y t i a m i n a y c o m i e n z a l a t r a n s c r i o p c i o n d e u n a d e l a s d o s c a d e n a s e n l a r e g i o n a
d y a c e n t e l a s r e g i o n e s p r o m o t o r a s e n s i n o s o n t r a n s c r i t a s d e n t r o d e u n a r e g i o n e s p e c i f i c a d e l d n a s o l o u n a d
e l a s d o s c a d e n a t i e n e s e n t i d o e s d e c i r e s t r a n c r i t a e n r n a p e r o e n o t r a r e g i o n d i s t i n t a d e e s a m i s m a m o l e c u l a
d e d n a l a o t r a c a d e n a s e r a l a q u e t e n g a s e n t i d o a p e s a r d e e s t o l a i n f o r m a c i o n p a r a e l a b o r a r c u a l q u i e r m o l e c
u l a d a d a d e r n a o c a d e n a p o l i p e p t i d i c a r e s i d e e x c l i s i v a m e n t e e n u n a d e l a s d o s c a d e n a s e s d e c i r q u e l a r n a p o
l i m e r a s a n o s a l t a d e u n a c a d e n a d e d n a a l a o t r a d u r a n t e e l p r o d e s o d e t r a n s c r i p c i o n d e u n g e n e n p a r t i c u l a r o
g r u p o d e g e n e s a d y a c e n t e s p a r a l a s i n t e s i s d e u n a m o l e c u l a d e r n a t a n t o l a m o l e c u l a d e r n a m c o m o l a d e r n a r s
e a s o c i a n c o n p r o t e i n a s f o r m a n d o p r e c u r s o r e s y q u e e n t o n c e s e s e d i r i g e n d e l n u b l e o a l c i t o p l a s m a a h i e l m e n
s a j e e s l e i d o u n i d i r e c c i o n a l m e n t e p o r u n o o m a s r i b o s o m a s p o l i s o m a s c o m e n z a n d o e n e l e x t r e m o s i c a d a u n o
d e l o s v e i n t e a m i n o a c i d o s s e r e c o n o c e p o r s u p r o p i o t i p o d e r n a t e n t o n c e s e n e l c i t o p l a s m a e x i s t e n u n m i n i m
o d e v e i n t e e s p e c i e s d e r n a t l a u n i o n d e u n a m i n o a c i d o c o n s u m o l e c u l a d e r n a t e s m e d i a d a p o r u n e n z i m a e s p e c
i f i c a e n u n p r o d e s o d e n o m i n a d o a c t i v a c i o n o c a r g a d o e n a l g u n a p a r t e d e l r n a t h a y u n a s e c u e n c i a d e t r e s n u c l
e o t i d o s e l a n t i c o d o n q u e e s e l c o m p l e m e n t o d e l c o d o n d e r n a m l a a f i n i d a d d e l a s t e r n a s c o m p l e m e n t a r i a s l l e
v a a c a d a a m i n o a c i d o a r e l a c i o n a r s e a d e c u a d a m e n t e c o n l o s o t r o s a m i n o a c i d o s d e l a c a d e n a p o l i e p t i d i c a e n
s i n t e s i s u n a e n z i m a r i b o s o m a l u n e e l g r u p o a m i n o y e l g r u p o c a r b o x i l o d e l o s a m i n o a c i d o s a d y a c e n t e s f o r m
a n d o e l e n l a c e p e p t i d i c o d e s p u e s d l a m o l e c u l a d e r n a t s e l i b e r a d e s u a m i n o a c i d o d e l r n a m d e l r i b o s o m a q u e
d a n d o l i b r e p a r a a c t i v a r s e o u n i r s e c o n o t r o a m i n o a c i d o t a m b i e n l i b r e d e l m i s m o t i p o c u a n d o e l r i b o s o m a l l
e g a a l f i n a l d e l m e n s a j e s e c o m p l e t a l a t r a d u c c i o n d e l c o d i g o n u c l e o t i d o e n u n a s e c u e n c i a d e a m i n o a c i d o s l o
s r i b o s o m a s b a c t e r i a n o s e s t a n c o m p u e s t o s d e d o s s u b u n i d a d e s p r i n c i p a l e s u n a s u b u n i d a d g r a n d e d e c i n c u
e n t a s y u n a s u b u n i d a d d e t r e i n t a s d o n d e s e s u n i d a d s v e d b e r g d e f l o t a c i o n u n c o e f i c i e n t e d e s e d i m e n t a c i o n
m o l e c u l a r e n u l t r a c e n t r i f u g a m a s d e t r e i n t a p r o t e i n a s d i f e r e n t e s e s t a n a s o c i a d a s c o n e l r n a r e n l o s r i b o s o
m a s p e r o a u n n o s e h a e l u c i d a d o l a f u n c i o n e s p e c i f i c a q u e l l e v a a c a b o a l p a r e c e r c u a n d o m e n o s h a y d o s s i t i o s
f u n c i o n a l e s e n e l r i b o s o m a e l p r i m e r o u n s i t i o p e p t i d a l y s e g u n d o u n s i t i o a m i n a c i l d u r a n t e l a s i n t e s i s d e p r
o t e i n a s e l r n a m s e u n a a l a s u b u n i d a d d e t r e i n t a s l a p r i m e r a m o l e c u l a d e r n a t a c t i v a d a e n t r a a l s i t i o p e p t i d a
l q u i z a p a s a n d o a t r a v e z d e l s i t i o a m i n o a c i l l a s i g u i e n t e m o l e c u l a d e r n a t c a r g a d a e n t r a a l s i t i o a m i n o a c i l y
e n c i m a t i c a m e n t e s e f o r m a u n e n l a c e p e p t i d i c o e n t r e l o s d o s a m i n o a c i d o s a d y a c e n t e s e l r n a t n o a c t i v a d o e s
e l s i t i o p e p t i d a l d e j a a h o r a e l r i b o s o m a y p u e d e r e s u l t a r e n z i m a t i c a m e n t e a c t i v a d o u n a v e z m a s c o n t r a o t r
a m o l e c u l a d e m i n o a c i d o d e s u m i s m a e s p e c i e e l c o m p l e j o r e s t a n t e r n a t d i p e p t i d o p a s a d e l s i t i o a m i n o a c i l a
l s i t i o p e p t i d a l c o n i c i d i e n d o c o n u n m o v i m i e n t o d e l r i b o s o m a j u n t o c o n e l m e n s a j e r o q u e e x p o n e e l s i g u i e n
t e c o d o n d e r n a m e n e l s i t i o v a c a n t e a m i n o a c i l e s t e p r o c e s o s e r e p i t e h a s t a q u e s e c o m p l e t a e l m e n s a j e s e p i e
n s a q u e c i e r t a s p r o t e i n a s e s p e c i f i c a s e s d e c i r f a c t o r e s d e l i b e r a c i o n r e c o n o c e n e s t o s c o d o n e s d e t e r m i n a c
i o n y s e p a r a n l a d c a d e n a p o l i p e p t i d i c a y a c o m p l e t a d e l a u l t i m a m o l e c u l a d e r n a t c a d a m o l e c u l a d e r n a t c o n
t i e n e d e s e t e n t a y c i n c o a o c h e n t a n u c l e o t i d o s e n u n o r d e n e s p c i f i c o l a t e r m i n a c i o n t r e s d e t o d a s l a s m o l e c u
l a s d e r n a t q u e s e u n e n a l o s a m i n o a c i d o s a l p a r e c e r t e r m i n a n e n c i t o c i n a c i t o c i a n a d e i n a e l e x t r e m o c i n c o t e
r m i n a e n u n r e s i d u o d e g u a n i n a e n e l r n a t s u e l e n p r e s e n t a r s e b a s e s p o **sin decifrar** d w a l l d w g v d g a d c q u w w d j e d l
t g f k p x u k z s g o v x x a h e e k c g x w a x f j j c l a u e o f h u w h c y e c v h f o m i c q m v d m b t t m f q l s l i k p b q k z s g w w p f r n i c s r t e i
d d c f d w x v o q c v b s q t s y z z j u f q b a f m r f r j s l d v d d j y e w l b u o n e k f o i p l q z d y w b m d x q a r i w g v d g b k v c w b m p l u z j u f

q b t l f z j h w u b d h q r c y e w m p x m r j u z o g e l a o l u k h h k u d h f i e c w t f a r k h a r b b y z r z e f o e t m g m f t w z h h w g z c u k g x b o q r k h s s g a u r h x k j o v p n a q t u y i b d h o t r j j c x h j d n s q t z x f o q t e q j s z x i z m f q h o k t u p z v d m b t s y x z j q k o l s y d m r j u c g i y z f r b s h x g h m z e j a q h s i z p l y r o n c u p d c q k c m g u e z j q k r x a l z z k i w o x a m u s z e v s k t w a m f s a a b t h f n l d g r h c x q r v k f o e p y z y z c s s l e y o h w y u o j j y m b k y n w k p f m l z d g o v x x a d j f w q b u c o n g q j o x a u z k r s w s g a u f d i c a b t r c a m k h w g i g c y z c e k q h s i z d j i a b l t h f h u e m f t r c x z u u f w g p u p d z d s i k p w u k r t w w g p a g z e y f o r j l m b z b y i t c c z z r t w w g p h a b f t a t b r u z o r h s b b c a g m r c a b h p w u c f f g f e d n m m k e k s v g y q p l u l s k b c z z e b s g b c n q r z i v s e p j d n k u a b t a u e o i e l s b c u e a r s l s k x u z z j q e s g j x a s z u f s g c z a q d y d a x i c a m z d s s g t f q w k h w a h c n q q d y f o e x h u b z q d a x c n q d j f j c u p v x d h k w s e r i p n e q v s g x h m t i q u w e v o m m z d s m j j c l z x k s b b c u g q r s a z z j u z h e q u i t s i e d r f s f x p u x o i y f q b e c a c v k f o f d f q b l b s a x c m m i v h s o v i o q b f c g s e p w f h m q v c k s y x z j y f h x h c e c v b s d k d n q h e q w b x a l z z d f g z b r c e s i e f w v d k g d t e v w y x w m o r h s a t h x q t e j a d h s y b n c y h s i i c p n j u d q h s i z z u u f w g p o d z t y d u n p h u m r g m s v d x u e z s s d t g u x z w e j a b a g q s z e f w g p j g d u u l s k b c z z i b s g b c n q r z i v s n c j a k z f w d m x x a d z d a q b p l q k j y y i b t h f d u u t w w d u c t v u d u k j j a m w e j a t a y z t e q e w g d u o h u e w j b i u x z w e j a t r c a m u u w b e p w q r g u h h b s c o n j f m s w t b m a v h m b t t h l h d q v s t y o e s v g m s l t j m q v b s t h t g u k d u l w h c c z z u u d c l t m j s i u e c l s y x z j f j c m t c z z j s g a i a y f z j q d u n c i e b f t g b x h j g d u u f h x c y d c z v w f x c n q r j y y b b u c o z u e k r x e y z c z u f r h s y e t g e k w v x i z d e b s a h a y o t c q e s g h u v d i q k w l t y z b v d l f t p f o n u e f o w t h u m r k j o v x f s t r d a b t p f o n d y w b s d x q k i d s a i j y p d z d a q b p l x z j y f h x h c e c v f j c m t c z z j i a g x t h o t v d l f t p f r h e q d r x t m f z d e d s v j f m l v d k o c t l m o l u v s t r n g z i s g a h u o x z c y r o w d l p d c q u o w t h m o v f l w w x w m o l u v s v p g n h r h k s e p y e o v s a t b r c p z u t w z v d x u f f w w b x i c o n r b s z m t l z z i s m o e f o u d i s g a i d h q m k u v s e p g m p l y f o k x u p d c u u h n g u u m t b m m x c x a k r i w b s x g m r i y t c l d g m r i d s h r g h m l r b y c w t u o k r h s q b d h q r j e t f x a u z n k q u w h c h d z d u k b k p g u s f s g b w g c m k e h s h x h h d z k h s b l r l u o k e j z t u c s t i q w g e p z u f l h s q t i i d b v s m o m g i p d v b d w u g i s d e u l w v p m o g r k e g x v o z c r u v w v x i z o r w a b t i l q b z u f h h h x a r c e k s k g i d d j g m s a p s q m v b l s q i i y d j y j j x c x q q v v w f g r c m o f h g h k d f m c f u k d x g i p d j f w f m p l e t z d l s k t m q m v i l c l i y j s f i q o j j y g r k u v s l h i z m l u k h k p m u f l u f h x v y z d i q u w h c s f h v d w b n c u s q r d j s l e i z r r r a z b s u p o f h v s e p h f d r i a e n t h a b f f a s g w u s z e b s h t g y m m n w g

5 Ejercicio 6

- Dar la matriz de cifrado explicando paso a paso como se obtiene incluyendo congruencias involucradas.

  Como hay asociaciones en pares podemos intuir que se utilizan diagramas. Entonces debemos encontrar la matriz:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

  Nos dan la siguiente relación

$$\begin{pmatrix} C \\ M \end{pmatrix} = \begin{pmatrix} 2 \\ 12 \end{pmatrix} \mapsto \begin{pmatrix} 2 \\ 20 \end{pmatrix} = \begin{pmatrix} C \\ U \end{pmatrix}$$

$$\begin{pmatrix} W \\ H \end{pmatrix} = \begin{pmatrix} 22 \\ 7 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 11 \end{pmatrix} = \begin{pmatrix} A \\ L \end{pmatrix}$$

$$\begin{pmatrix} M \\ K \end{pmatrix} = \begin{pmatrix} 12 \\ 10 \end{pmatrix} \mapsto \begin{pmatrix} 4 \\ 18 \end{pmatrix} = \begin{pmatrix} E \\ S \end{pmatrix}$$

$$\begin{pmatrix} E \\ W \end{pmatrix} = \begin{pmatrix} 4 \\ 22 \end{pmatrix} \mapsto \begin{pmatrix} 18 \\ 4 \end{pmatrix} = \begin{pmatrix} S \\ E \end{pmatrix}$$

$$\begin{pmatrix} D \\ S \end{pmatrix} = \begin{pmatrix} 3 \\ 18 \end{pmatrix} \mapsto \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} D \\ E \end{pmatrix}$$

$$\begin{pmatrix} F \\ G \end{pmatrix} = \begin{pmatrix} 5 \\ 5 \end{pmatrix} \mapsto \begin{pmatrix} 17 \\ 8 \end{pmatrix} = \begin{pmatrix} R \\ I \end{pmatrix}$$

$$\begin{pmatrix} R \\ Q \end{pmatrix} = \begin{pmatrix} 17 \\ 16 \end{pmatrix} \mapsto \begin{pmatrix} 21 \\ 0 \end{pmatrix} = \begin{pmatrix} V \\ A \end{pmatrix}$$

$$\begin{pmatrix} T \\ J \end{pmatrix} = \begin{pmatrix} 19 \\ 9 \end{pmatrix} \mapsto \begin{pmatrix} 13 \\ 3 \end{pmatrix} = \begin{pmatrix} N \\ D \end{pmatrix}$$

$$\begin{pmatrix} K \\ U \end{pmatrix} = \begin{pmatrix} 10 \\ 20 \end{pmatrix} \mapsto \begin{pmatrix} 4 \\ 4 \end{pmatrix} = \begin{pmatrix} E \\ E \end{pmatrix}$$

$$\begin{pmatrix} I \\ P \end{pmatrix} = \begin{pmatrix} 8 \\ 15 \end{pmatrix} \mapsto \begin{pmatrix} 18 \\ 19 \end{pmatrix} = \begin{pmatrix} S \\ T \end{pmatrix}$$

$$\begin{pmatrix} D \\ Q \end{pmatrix} = \begin{pmatrix} 3 \\ 16 \end{pmatrix} \mapsto \begin{pmatrix} 17 \\ 20 \end{pmatrix} = \begin{pmatrix} R \\ U \end{pmatrix}$$

$$\begin{pmatrix} A \\ J \end{pmatrix} = \begin{pmatrix} 0 \\ 9 \end{pmatrix} \mapsto \begin{pmatrix} 2 \\ 19 \end{pmatrix} = \begin{pmatrix} C \\ T \end{pmatrix}$$

$$\begin{pmatrix} S \\ N \end{pmatrix} = \begin{pmatrix} 18 \\ 13 \end{pmatrix} \mapsto \begin{pmatrix} 20 \\ 17 \end{pmatrix} = \begin{pmatrix} U \\ R \end{pmatrix}$$

$$\begin{pmatrix} K \\ C \end{pmatrix} = \begin{pmatrix} 10 \\ 2 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 18 \end{pmatrix} = \begin{pmatrix} A \\ S \end{pmatrix}$$

$$\begin{pmatrix} W \\ H \end{pmatrix} = \begin{pmatrix} 22 \\ 7 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 11 \end{pmatrix} = \begin{pmatrix} A \\ L \end{pmatrix}$$

$$\begin{pmatrix} Y \\ Y \end{pmatrix} = \begin{pmatrix} 24 \\ 24 \end{pmatrix} \mapsto \begin{pmatrix} 6 \\ 4 \end{pmatrix} = \begin{pmatrix} G \\ E \end{pmatrix}$$

$$\begin{pmatrix} P \\ B \end{pmatrix} = \begin{pmatrix} 15 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 17 \end{pmatrix} = \begin{pmatrix} B \\ R \end{pmatrix}$$

$$\begin{pmatrix} Q \\ Y \end{pmatrix} = \begin{pmatrix} 16 \\ 24 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 8 \end{pmatrix} = \begin{pmatrix} A \\ I \end{pmatrix}$$

$$\begin{pmatrix} O \\ E \end{pmatrix} = \begin{pmatrix} 14 \\ 4 \end{pmatrix} \mapsto \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} C \\ A \end{pmatrix}$$

$$\begin{pmatrix} C \\ T \end{pmatrix} = \begin{pmatrix} 2 \\ 19 \end{pmatrix} \mapsto \begin{pmatrix} 18 \\ 3 \end{pmatrix} = \begin{pmatrix} S \\ D \end{pmatrix}$$

$$\begin{pmatrix} G \\ O \end{pmatrix} = \begin{pmatrix} 6 \\ 14 \end{pmatrix} \mapsto \begin{pmatrix} 4 \\ 2 \end{pmatrix} = \begin{pmatrix} E \\ C \end{pmatrix}$$

$$\begin{pmatrix} A \\ L \end{pmatrix} = \begin{pmatrix} 0 \\ 11 \end{pmatrix} \mapsto \begin{pmatrix} 14 \\ 3 \end{pmatrix} = \begin{pmatrix} O \\ D \end{pmatrix}$$

$$\begin{pmatrix} Q \\ I \end{pmatrix} = \begin{pmatrix} 16 \\ 8 \end{pmatrix} \mapsto \begin{pmatrix} 8 \\ 6 \end{pmatrix} = \begin{pmatrix} I \\ G \end{pmatrix}$$

Trabajaremos con la la transformación 19, por lo que quedaría de la siguiente manera.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 2 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 14 \\ 4 \end{pmatrix} \pmod{26}$$

Resultando las siguientes congruencias:

$$2a + 0b \equiv 14 \pmod{26} \mapsto a \equiv 7 \pmod{13}$$
$$2c + 0d \equiv 4 \pmod{26} \mapsto c \equiv 2 \pmod{13}$$

Ahora obtendremos su inverso para saber su valor exacto, por lo que nos resulta lo siguiente:

$$mcd(1, 13) \mapsto 1 = 1(14) - 13(1) \mapsto 7 = 1(98) - 13(7) \mapsto 11^{-1} \equiv 98 \pmod{13} = 7$$

$$mcd(1, 13) \mapsto 1 = 1(14) - 13(1) \mapsto 2 = 1(28) - 13(2) \mapsto 11^{-1} \equiv 28 \pmod{13} = 2$$

Ahora utilizamos las transformaciones 9 y 21, esto para poder encontrar el valor de b y d. Entonces los sistemas nos queda de la siguiente manera.

$$4a + 2b \equiv 6 \pmod{26} \tag{1}$$

$$4c + 2d \equiv 2 \pmod{26} \tag{2}$$

$$4a + 4b \equiv 10 \pmod{26} \tag{3}$$

$$4c + 4d \equiv 20 \pmod{26} \tag{4}$$

Restando la congruencia 1 con la 3 y la 2 con la 4 obtenemos las siguientes congruencias:

$$-2b \equiv -6 \pmod{26} \mapsto -b \equiv -2 \pmod{13} \tag{5}$$

$$-2d \equiv -18 \pmod{26} \mapsto -d \equiv -7 \pmod{13} \tag{6}$$

Y al buscar el inverso multiplicativo no resulta lo siguiente:

$$mcd(1, 13) \mapsto 1 = -1(-14) - 13(1) \mapsto 2 = 1(-28) - 13(2) \mapsto 11^{-1} \equiv -28 \pmod{13} = -2$$

$$mcd(1, 13) \mapsto 1 = -1(-14) - 13(1) \mapsto 7 = 1(-98) - 13(7) \mapsto 11^{-1} \equiv -98 \pmod{13} = -7$$

Por lo que la matriz de cifrado es:

$$\begin{pmatrix} 7 & -2 \\ 2 & -7 \end{pmatrix}$$