

Tarea 1 Criptografia

Victor Hugo Gallegos Mota
316160456

José Demian Jiménez
314291707

Carlos Cruz Rangel
314208682

13 de septiembre del 2022

1 Problema 1

Explique brevemente porque en \mathbb{Z}_n dados $a \cong b \pmod{n}$ y $c \cong d \pmod{n}$, se tiene que $ac \cong bd \pmod{n}$

P.D $a \cong b \pmod{n}$ y $c \cong d \pmod{n}$ se tiene que $ac \cong bd \pmod{n}$

Suponer que $a \cong b \pmod{n}$ y $c \cong d \pmod{n}$

Puesto que $a \cong b \pmod{n}$, $\exists k \in \mathbb{Z}$ tal que $a - b = kn$

Puesto que $c \cong d \pmod{n}$, $\exists r \in \mathbb{Z}$ tal que $c - d = rn$

Luego tenemos que $ac - bd = ac - cb + cb - bd$

$$= c(a - b) + b(c - d)$$
$$= c(kn) + b(rn)$$
$$= (ck + br)n \text{ donde } ck + br \in \mathbb{Z}$$

Por lo tanto $ac \cong bd \pmod{n}$

2 Problema 2

2) Resuelva el siguiente sistema de congruencia en caso de tener solución, en caso contrario justifique por que no tiene solución.

$$x \cong 25 \pmod{35}$$

$$x \cong 15 \pmod{65}$$

$$x \cong 10 \pmod{15}$$

$$x \cong 35 \pmod{55}$$

$$x \cong 55 \pmod{85}$$

No tiene solución, veamos por que:

Pd.- Sea el sistema de congruencias A, A no tiene solución.

Dem.- Sea A el siguiente sistemas de congruencias:

$$x \cong 25 \pmod{35}$$

$$x \cong 15 \pmod{65}$$

$$x \cong 10 \text{mod}(15)$$

$$x \cong 35 \text{mod}(55)$$

$$x \cong 55 \text{mod}(85)$$

Veamos si tienen solución por separado, si el $\text{mcd}(a, n)$ divide a "b" entonces tiene solución:

$$x \cong 25 \text{mod}(35) \quad \text{mcd}(1, 35) = 1, \text{ y } 1 \text{ divide a } 25, \text{ entonces cumple.}$$

$$x \cong 15 \text{mod}(65) \quad \text{mcd}(1, 65) = 1, \text{ y } 1 \text{ divide a } 15, \text{ entonces cumple.}$$

$$x \cong 10 \text{mod}(15) \quad \text{mcd}(1, 15) = 1, \text{ y } 1 \text{ divide a } 10, \text{ entonces cumple.}$$

$$x \cong 35 \text{mod}(55) \quad \text{mcd}(1, 55) = 1, \text{ y } 1 \text{ divide a } 35, \text{ entonces cumple.}$$

$$x \cong 55 \text{mod}(85) \quad \text{mcd}(1, 85) = 1, \text{ y } 1 \text{ divide a } 55, \text{ entonces cumple.}$$

Ahora veamos que tienen solución en conjunto, el teorema chino nos dice:

"Supongamos que n_1, n_2, \dots, n_k son enteros positivos coprimos dos a dos.

Entonces, para enteros dados a_1, a_2, \dots, a_k , existe un entero x que resuelve el sistema de congruencias simultáneas

$$x \equiv a_1 \pmod{n_1} \quad x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2} \quad x \equiv a_2 \pmod{n_2}$$

$$\vdots \qquad \qquad \qquad \vdots$$

$$x \equiv a_k \pmod{n_k} \quad x \equiv a_k \pmod{n_k}$$

Más aún, todas las soluciones x de este sistema son congruentes módulo el producto

$$N = n_1 n_2 \dots n_k \quad N = n_1 n_2 \dots n_k.$$

De manera más general, las congruencias simultáneas pueden ser resueltas si los n_i 's son coprimos a pares." entonces veamos si son coprimos.

$$\text{mcd}(35, 65) = 5 \text{ como los divide } 5 \text{ y } 1 \text{ no son coprimos.}$$

$$\text{mcd}(35, 15) = 5 \text{ como los divide } 5 \text{ y } 1 \text{ no son coprimos.}$$

$$\text{mcd}(35, 55) = 5 \text{ como los divide } 5 \text{ y } 1 \text{ no son coprimos.}$$

$$\text{mcd}(35, 85) = 5 \text{ como los divide } 5 \text{ y } 1 \text{ no son coprimos.}$$

$$\text{mcd}(65, 15) = 5 \text{ como los divide } 5 \text{ y } 1 \text{ no son coprimos.}$$

$$\text{mcd}(65, 55) = 5 \text{ como los divide } 5 \text{ y } 1 \text{ no son coprimos.}$$

$$\text{mcd}(65, 85) = 5 \text{ como los divide } 5 \text{ y } 1 \text{ no son coprimos.}$$

$$\text{mcd}(15, 55) = 5 \text{ como los divide } 5 \text{ y } 1 \text{ no son coprimos.}$$

$$\text{mcd}(15, 85) = 5 \text{ como los divide } 5 \text{ y } 1 \text{ no son coprimos.}$$

$$\text{mcd}(55, 85) = 5 \text{ como los divide } 5 \text{ y } 1 \text{ no son coprimos.}$$

Como no son coprimos entonces no tiene solución.

\implies El sistema A no tiene solución.

3 Problema 3

El siguiente texto fue cifrado en mono alfabetico, realice un análisis de frecuencias tomando en cuenta que los caracteres están en correspondencia de la siguiente forma $a=0, \dots, z=25$, no hay acentos ni ñ. Encuentre la clave y descifre el mensaje.

MENSAJE CIFRADO:

IL NPMTRFKL QNFHR ERI QLPQSMVEMQ QR RQTL LELNTLKEM ERAFEM L
NPRQFMKRQ QRIRSTFVLQ
IL RQSLIL CIMALI ER IL NLKERJFL ER SMVFE DL ERJMQTPLEM IL RVMIUSFMK
ERI QLPQSMVEMQ Y ILQ SILVRQ ER LELNTLSFMK. ERQNURQ ER SLTMPSR
JRQRQ ERQER IL ERSILPLSFMK ER IL NLKERJFQ, JUITFNIRQ VLPFLKTRQ
DLK QUPCFEM Y QR DLK BFGLEM RK IL NMAILSFMK DUJLKL CPLSFLQ
L RXTPFKQRSQ NPRQFMKRQ QRIRSTFVLQ QF KM TLJAFRK L IL SLNLS-
FELE JUTLSFMKLI FKDRPKRTR ERI VFPUQ. LOUF LNIFSLJMQ UKL NPURAL
ER RVMIUSFMK ER QUQFTUSFMK KRUTPL L IL NPMTRFKL ER NFSM ER
IL NPMTRFKL MJFSPMK Y QR SMJNLPM L IL RVMIUSFMK KRUTPL ER IL
VLPFRKTR ER NPRMSUNLSFMK ER IMQ ERJLQ. PRLIFZLJMQ SMJNLPLSFMKRQ
RKTPR ILQ FKTRPLSSFMKRQ RKTPR ILQ NPMTRFKLQ Q ER IMQ SMV(LIBL,RTL,CLJJL,ERITL
Y MJFSPMK) Y RI PRSRNTMP LSREM. IMQ LJFKMLSFEMQ SMJNLPTFEM
RKTPR TMELQ ILQ NPMTRFKLQ Q OUR QR UKRK L LSREM NRPJLKRSRK
SMKQTLKTRQ IM OUR FKEFSL OUR RQTMQ LJFKMLSFEMQ QMK RQRKS-
FLIRQ NLPL IL UKFMK NPRSFQL LI PRSRNTMP. IMQ SMJNIRGMQ PAE NLPL
SLEL VLPFLTR SMK RI PRSRNTMP QR UTFIFZLPMK NLP FERKTFBFSPL IMQ
LJFKMLSFEMQ FKVMIOUSPLEMQ RK IL FKTRPLSSFMK NPMTRFKL NPMTR-
FKL. IL PAE ER MJFSPMK RQTLAIRSR MSDRCTL Y EMQ SMKTLSTMQ BPRKTR
L IMQ QRQRKTLYSULPTM ER IL NPMTRFKL MPFCFKLI ER WUDLK NMP IM
TLKTM, RI KUJRPJ JREFM ER SMKTLSTMQ NMP PRQFEUMQ RQ JLYMP
NMP IM OUR RI SMKTLSTM TRPJMEFKLJFSM RQ JLQ RQTLAIR. IMQ PAE ER
IMQ SMV QMK QFJFILPRQ RK QRSURKSFL Y RQTPUSTUPL QFK RJALPCM,
RI PAE ER MJFSPMK NPRQRKTL IL ERQVFLSFMK JLQ CPLKER ER IL RQT-
PUSTUPL NMP UKM NUKTM MKSR LPJQE, SLUQLEM NMP UK SMKGUKTM
ER JUTLSFMKRQ SRPSLKLQ L IL CIFSMQFILSFMK KTPRQFTKRM SULPRKTL
Y TPRQ ER IL NPMTRFKL MJFSPMK Q QMK EFBPRKTR ER IL NPMTRFKL
MPFCFKLI OUR NPMVMSLK UK PRSMKMSFJFRKTM PREUSFEM NMP NLPT
ER IMQ LKTFURPNMQ KRUTPLIFZLKTRQ. KURQTPMQ PRQUITLEM QU-
CUFRPRK OUR ILQ NPRQFMKRQ QRIRSTFVLQ QMK FKEUSFELQ NMP IL
VLSUKLSFMK JLQFVL RK TMEM RI JUKEM Y NMP NRPQFQTRKSFL ER FK-
BRSSFMQR PRSUPPRKTRQ RK FKEFVFEUMQ FKJUKMERNPFJFEMQ, OUR
KM RIFJFKLPMK IL FKBRSSFMK Y LSLALPMK BLSFIFTLKEM IL QRIRSSFMK
ER VFPUQ SUYLQ SLPLSTRPFQTFSLQ QMK EFBPRKTRQ L IMQ SMV LK-
TRPFMPRQ, JRKM NLTMCCKMQ NRPM SMK JLYMP TPLKJFQFAFIFELE.

Lo primero fue implementar un script en python que nos calculara las frecuencias ordenando de mayor a menor segun su porcentaje y aparicion

```

def frecuencias(archivo):
    f = open(archivo, 'r') # abrir el archivo
    text = f.readlines()
    # Lista con 3 valores Letra / Frecuencia / Porcentaje
    l = [[chr(65+i), 0, ''] for i in range(26)]
    total = 0 # total de letras
    for line in text:
        for char in line:
            if (char == ' ' or char == '\n' or char == '.'):
                continue
            else:
                l[ord(char)-65][1] += 1 # Aumentar frecuencia
                total += 1
    for i in range(len(l)):
        # Porcentaje
        l[i][2] = (l[i][1]*100) / total
        l[i][2] = format(l[i][2], '.2f') # 2 decimales
    l.sort(key=lambda x: x[1], reverse=True) #De mayor a menor
    return l
def main():
    print("Letra\tFrecuencia\tPorcentaje") #Imprime tabla
    for i in frecuencias("archivo.txt"):
        print(i[0], '\t', i[1], '\t\t', i[2], '%')
if __name__ == '__main__':
    main()

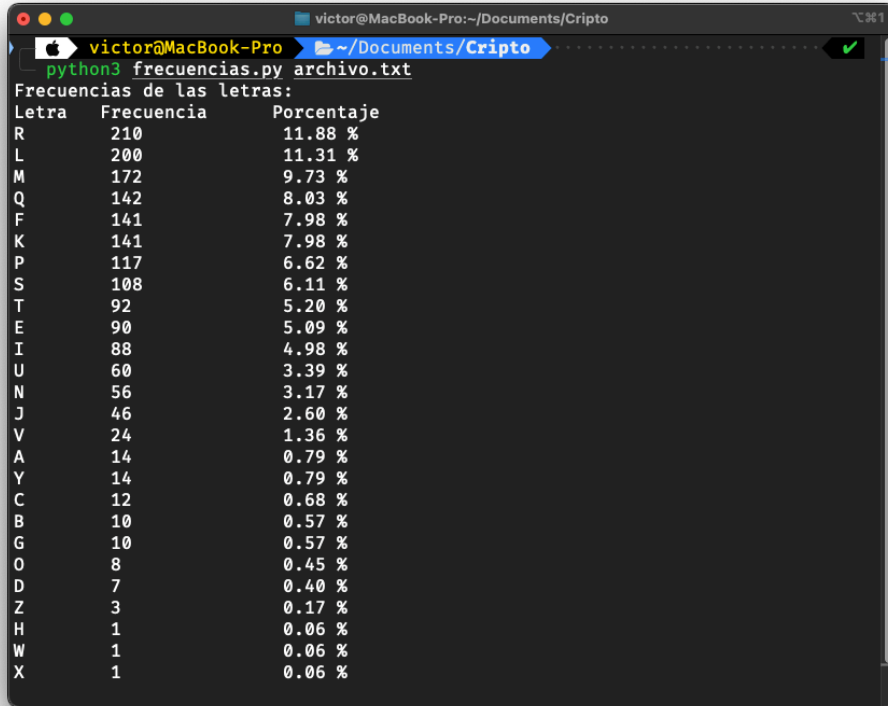
```

Estamos hablando de valores estadísticos probaremos solo a sustituir los dos caracteres más frecuentes en el texto cifrado por los dos caracteres más frecuentes en español teniendo en cuenta que el problema indica que no se contemplen acentos ni ñ. Entonces R = e y L = a, esto nos ayudara a identificar en el texto palabras que puedan ser comunes en español pero aun no logramos descifrar el mensaje, lo siguiente a realizar es identificar las palabras "cortas" de 2 o 3 letras pues son muy utilizadas en nuestro idioma en este caso comenzamos identificando a las letras *QMK* cambiandolas por *son* otro caso fue el de *OUR* el cual ya tenia su primer cambio *OUe* por lo que procedimos a cambiar *OU* por *PO* respectivamente posteriormente pasamos a palabras con 2 letras como fue el caso se *IL* cambiandolas por *la* respectivamente y asi cotinuamos probando una y otra vez iterando sobre cada palabra que lograba hacer sentido con una palabra real, hasta lograr sustituir todas las letras del abecedario por las siguientes

A	B	C	D	E	F	G	H	I	J	K	L	M
b	f	g	h	d	i	j	k	l	m	n	a	o

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
p	q	r	s	e	c	t	u	v	w	x	y	z

Implementamos un metodo llamado sustitucion el cual lee el texto en un



```
victor@MacBook-Pro: ~/Documents/Cripto
python3 frecuencias.py archivo.txt
Frecuencias de las letras:
Letra  Frecuencia  Porcentaje
R      210        11.88 %
L      200        11.31 %
M      172        9.73 %
Q      142        8.03 %
F      141        7.98 %
K      141        7.98 %
P      117        6.62 %
S      108        6.11 %
T      92         5.20 %
E      90         5.09 %
I      88         4.98 %
U      60         3.39 %
N      56         3.17 %
J      46         2.60 %
V      24         1.36 %
A      14         0.79 %
Y      14         0.79 %
C      12         0.68 %
B      10         0.57 %
G      10         0.57 %
O      8          0.45 %
D      7          0.40 %
Z      3          0.17 %
H      1          0.06 %
W      1          0.06 %
X      1          0.06 %
```

Figure 1: Resultado en consola al ejecutar el script anterior

archivo .txt en nuestro script principal para susituir cada letra MAYUSCULA por minusculas para identificar mejor y obtener asi el mensaje descifrado

```
def sustitucion(archivo):
    f = open(archivo, 'r')
    text = f.readlines()
    for line in text:
        for char in line:
            if char == 'R':
                print('e', end='')
            elif char == 'L':
                print('a', end='')
            elif char == 'Q':
                print('s', end='')
            elif char == 'M':
                print('o', end='')
            elif char == 'K':
```

```

        print('n', end='')
    elif char == 'I':
        print('l', end='')
    elif char == 'E':
        print('d', end='')
    elif char == 'O':
        print('q', end='')
    elif char == 'B':
        print('f', end='')
    elif char == 'T':
        print('t', end='')
    elif char == 'C':
        print('g', end='')
    elif char == 'J':
        print('m', end='')
    elif char == 'F':
        print('i', end='')
    elif char == 'S':
        print('c', end='')
    elif char == 'P':
        print('r', end='')
    elif char == 'N':
        print('p', end='')
    elif char == 'U':
        print('u', end='')
    elif char == 'Y':
        print('y', end='')
    elif char == 'A':
        print('b', end='')
    elif char == 'V':
        print('v', end='')
    elif char == 'D':
        print('h', end='')
    elif char == 'G':
        print('j', end='')
    elif char == 'H':
        print('k', end='')
    elif char == 'Z':
        print('z', end='')
    elif char == 'X':
        print('x', end='')
    elif char == 'W':
        print('w', end='')
    else:
        print(char, end='')
f.close()

```

```

def main():
    # Mostrar el texto con las letras sustituidas
    print("Texto con las letras SUSTITUIDAS: \n")
    sustitucion("archivo.txt")
if __name__ == '__main__':
    main()

```

MENSAJE DESCRIFRADO:

la proteina spike del sarscovdos se esta adaptando debido a presiones selectivas la escala global de la pandemia de covid ha demostrado la evolucion del sarscovdos y las claves de adaptacion. despues de catorce meses desde la declaracion de la pandemis, multiples variantes han surgido y se han fijado en la poblacion humana gracias a extrinsecas presiones selectivas si no tambien a la capacidad mutacional inherente del virus. aqui aplicamos una prueba de evolucion de sustitucion neutra a la proteina de pico de la proteina omicron y se comparo a la evolucion neutra de la variante de preocupacion de los demas. realizamos comparaciones entre las interacciones entre las proteinas s de los cov(alfa,eta,gamma,delta y omicron) y el receptor acedos. los aminoacidos compartido entre todas las proteinas s que se unen a acedos permanecen constantes lo que indica que estos aminoacidos son esenciales para la union precisa al receptor. los complejos rbd para cada variante con el receptor se utilizaron para identificar los aminoacidos involucrados en la interaccion proteina proteina. la rbd de omicron establece ochenta y dos contactos frente a los sesentaycuatro de la proteina original de wuhan por lo tanto, el numero medio de contactos por residuos es mayor por lo que el contacto termodinamico es mas estable. los rbd de los cov son similares en secuencia y estructura sin embargo, el rbd de omicron presenta la desviacion mas grande de la estructura por uno punto once rmsd, causado por un conjunto de mutaciones cercanas a la glicosilacion. cuarenta y tres de la proteina omicron s son diferente de la proteina original que provocan un reconocimiento reducido por parte de los anticuerpos neutralizantes. nuestros resultados sugieren que las presiones selectivas son inducidas por la vacunacion masiva en todo el mundo y por persistencia de infecciones recurrentes en individuos inmunodeprimidos, que no eliminaron la infeccion y acabaron facilitando la seleccion de virus cuyas características son diferentes a los cov anteriores, menos patógenos pero con mayor transmisibilidad.

4 Problema 4

El siguiente cifrado es implementado en vigenere los caracteres fueron puestos en una biyeccion del 0 al 25 donde a=0 y z=25 sin signos de puntuacion ni ñ. Aplique la prueba de kasiski de la longitud de la clave, la clave y despues decifre el mensaje.

P N X ARW U Z I E W A L M A Z R T M Y Z D B I E P A E Q M
LEE U V W A Z Z B L G T Z E L L H A C Z C H A C P L H A E
Z J H A Q P M B B V L Q N M L L E L B N X E W Q B N A E D N

OEL X H P S E W F W A O I Y Z S L M P L L H A R D T B Z N
WEL P N N E V Z R A E E W F P X M Q R Y D X G Y Z S L W O
LHT A G L T K I A D F H Z Z L R E I R D C T A N N A U M Y
WEK I Q P M B B V L E G C A P D B N V N I H L R Q A G B N
DIT L R G A K Q B D P B A B D C H V E F L H A E T S H A P
LIK M Y P S R Z B D E M W A P S E W U Z R G M N O U K I A
EET T T F N T A U Z R T A R Y E E A R N A W W E J D X A C
FEL T B C O V Q N N O G A V P T X T V E R H A Q P L T K N
AAK I Q L R E M S T R F M M L Y L W F E E G I F F C K M N
NIH V R W D B I Q P L T J B O A F Q G T A E T R R O T V H
PSM Z N N A L I P Z N N V C P I G I Q Z Q N M Z P D B I Q
ZSF M G C O L L R L L M C E L S X D R T A B U C C E L Q B
YAG B R N U T V Q Z A U Z V X O L T N A U X Z G L P T Z N
DAE Q E D E X A P F C A W H Y Z N U O T D H I Y W E O I A
EAK T N G I L B N L L V Q R W O W M F N U U Z V X O L C A
MIV P B B U X A R L C X Z P L B T D B W A G L B L T H L N
GEE W P T D T L D F E X A R D O I Z R R U G B B X I F I Z
LYH A R W O J C R P S T K Y L R X B E T U G N N W C N I A
OOE W C F D X L V D T B V T F I K U N D D X K R C C T M F
FNF I L L T X G R D O J C R P S B V G P R K W T Z M B P R
CMT V N F N F I L L T X T R D I G N B C M X M F F N T M F
AEV Q R O E X A P L R T J N U O I M E Z U G X B N O F I F
CEV P B Y C A W R W M T G N E E X Z N O E E U V D M H K B
WOK Z B U O U Z V W L T V G P Q N M R W C T J R W L H L R
XIM Q N P L B V F P C M W I Z L H M A A I V I Q L Y S I B
DES I Z M U E T B P N X T C P I G I Q Z A R Y H P A L K B
RRB B B X I F I Z L A R Y H P S N A G Z B X Z E P O F Q U
PRF I A L A R Y H P B T Z O L R B L N O S X P V D T X Z V
KOF Q G T A J C V E E G U R W O I M E Z S B V Q P S V W Z
AOG M E P L I M V Y A W W N O V B Z G T O G W F L S H U N
XOL B R X E K W F Z S T T N D P K W S F N W Q Q L D X A Q
PEL I F P L O I E Z J T G N W O O Q Q T J H U V A A I I R
DTT C A A O V W N E U K L V O O R U N C E T L B A O K M Y
ZLH Z Q P L T T N N A L I Y O E T P V P L F I L L T X V B


```

ZBX L R N I H T R X E M Q Z Z S N V Y L P B H U F R Z I Z
ZSV W A P L W M Q Z L X A B A L T U B D Y G I Q L E E X R
TNT L B D E Z C V L I G B N N T H I Q P N M Z B O E G I Q
LVT T V P R H V F F P E Q P L S T U R Y A S I F Y I E W F
XAL Z H O O L X E Z C X L V X I X V G Z S G Q Z Z D H A R
TMI I P T E G B B X I I I C L S X V B D H T K R E A K L R
EEG L E L S J C R T R V W A P S H U V E I T I H Y Q N M A
PRO Q B D A L I O T A J C R Y O M M A T A H B E L A E B R
CNT B V G A E I S T E L B N E R T V F N U K Z V L N H Z Z
LLF M A E E I M E Z M B B V L S X A B M R X A N W T T J N
LCT L N C A M W P F A G L B E E K U V Y A F W F O E V M A
LRR M Z A E S W Y L M N A V N A F Q G T A T P B R O N V T
CIM W D F E M M C L S T T R A R X O H Y T X K E P O J C R
PLX A P L R T J N U O X A G L B T Q Y L N W W F F S N Z E
ZMX I F Z M X I Y A E B V N O O R M S P C M Q I L M X V G
PEE M F N A K I O L J H Z B U O X A G L B T J N T L T V Q
ZEE X E T M X Z I L L L L R W A G W P S E H J F P R O M S
LSV Q A L D H Y H P E E U R C E G O H P D X T C L S M M Y
OEU W Q L S M M A T A Z Z N Y D X A F P M X R N Y Z T A P
NXN T C P I G I Q Z D X U V E I T T Y P G H M Y X O F M A
EOW M S P L B K V E A K I Y Z S G W I T O L U V E I T A R
WEO I A E O V W Z Z T H L B D Y T T N M R T H N C A E I A
ZVB I M K E E M F N A K I O L J H L R N I W Q B G O E I E
PNX T V Y E K Q B C D X T C P I G I Q Z Q N M R D E L M E
FIW W C C E Z C A E O E I A Z V B I N W G H I F F S M I Q
LPT X R N E J C R G I X V R O E M C P L B X H N E I T M F
XIT X N C A M W C L R T T N D O K L R C A K M F A O G L V
ZEE T N N O G C A L S H V E T S T L R A A G Q P Z \

```

En este caso usaremos el siguiente algoritmo para poder sacar las cadenas que mas se repiten junto con la longitud de las mismas para asi poder tener una aproximacion de la longitud de la cadena.

```

mensaje = ""
PNXARWUZIEWALMAZRMZYDBIEPAEQM
LEEUVWAZZBLGTZELLHACZCHACPLHAE
ZJHAQPMBBVLQNMLLELBNXEQBNAEDN
OELXHPSEWFWAQIYZSLMPLLHARDTBZN
WELPNNEVZRAEEWFPXMQRDXGYZSLWO
LHTAGLTKIADFHZZLREIRDCTANNAUMY
WEKIQPMBBVLEGCAPDBNVNIHLRQAGBN
DITLRGAKQBDBABDCHVEFLHAETSHAP
LIKMYPSRZBDEMWAPSEWUZRGMNOKIA
EETTTFNZTAUZRRTARYEEARNWWEJDXAC
FELTBCOVQNNOGAVPTXTVERHAQPLTKN
AAKIQLREMSTRFMMLYLWFEEGIFCKMN
NIHVRWDBIQPLTJBOAFQGTAEOTRVH

```

PSMZNNALIPZNNVCPIGIQZQNMZPDBIQ
ZSFMGCOLLRLLMCELSXDRTABUCCELQB
YAGBRNUTVQZAUZVXOLTNAUXZGLPTZN
DAEQEDEXAPFCAWHYZNUOTDHIYWEIOIA
EAKTNGILBNLLVQRWOWMFNUUZVXOLCA
MIVPBBUXARLCXZPLBTDBWAGLBLTHLN
GEEWPTDTLDFEXARDOIZRRUGBBXIFIZ
LYHARWOJCRPSTKYLRXBETUGNNWCNIA
OOEWCDFXLVDTBVTFIKUNDDXKRCCTMF
FNFILLTXGRDOJCRPSBVGPRKWTZMBPR
CMTVNFNFILLTXTRDIGNBCMXMFFNTMF
AEVQROEXAPLRTJNUOIMEZUGXBNOFIF
CEVPBYCAWRWMTGNEEXZNOEEUVDMHKB
WOKZBUOUZVWLTVGPQNMWCTJRWLHLR
XIMQNPLBVFPCMWIZLHMAAIVIQLYSIB
DESIZMUETBPNXTCPIGIQZARYHPALKB
RRBBBXIFIZLARYHPSNAGZBXZEPOFQU
PRFIALARYHPBTZOLRBLNOSXPVDTXZV
KOFQGTAJCVEEGURWOIMEZSBVQPSVWZ
AOGMEPLIMVYAWWNOVBZGTOWFLSHUN
XOLBRXEKWFZSTNDPKWSFNWQQLDXAQ
PELIFPLOIEZJTGNWOOQQTJHUVAAIIR
DTTCAAOVWNEUKLVOORUNCETLBAOKMY
ZLHZQPLTTNNALIYOETPVPLFILLTXVB
ZBXLRNHTRXEMQZZSNVYLPBHUFZRIZ
ZSVWAPLWMQZLXABALTUBDYGIQLEEXR
TNTLBDEZCVLIGBNNTHIQPNMZBOEGIQ
LVTTVPRHVFFPEQPLSTURYASIFYIEWF
XALZHOOLEXEZCXLVXIXVGZSGQZZDHAR
TMIIPTEGBBXIIICLSXVBDHTKREAKLR
EEGLELSJCRTRVWAPSHUVEITIHYNMA
PROQBDALIOTAJCRYOMMATAHBELAEBR
CNTBVGAEISTELBNERTVFNUKZVLNHZZ
LLFMAEEIMEZMBBVLSXABMRXANWTTJN
LCTLNCAMWPFAGLBEEKUVYAFWFOEVMA
LRRMZAESWYLMNAVNAFQGTATPBRONVT
CIMWDFEMMCLSTRARXOHYTXKEPOJCR
PLXAPLRTJNUOXAGLBTQYLNWFFSNZE
ZMXIFZMXIYAEBVNOORMSPCMQILMXVG
PEEMFNAKIOLJHZBUOXAGLBTJNTLTVQ
ZEEXETMXZILLLLRWAGWPSEHJFPROMS
LSVQALDHYHPEEURCEGOHPDXTCLSMY
OEUWQLSMMATAZZNYDXAFPMXRNYZTAP
ZNXTCPIGIQZDXUVEITTPGHMYXOFMA
EOWMSPLBKVEAKIYZSGWITOLUVEITAR
WEOIAEOVWZZTHLBDYTTNMRTHNCAEIA

```

ZVBIMKEEMFNAKIOLJHLRNIWQBGOEIE
PNXTVYEKQBCDXTCPIGIQZQNMDELME
FIWWCCEZCAEOEIAZVBINWGHIFFSMIQ
LPTZRNEJCRGIXVROEMCPLBXHNEITMF
XITXNCAMWCLRTTNDOKLRCAKMFAOGLV
ZEETNNOGCALSHVETSTLRAGQPZ"

```

```

def ourrenciascadenas(l):
    mensaje = ''
    ln = len(l)
    for i in range(ln - 1):
        n = l[i + 1] - l[i]
        mensaje += str(n)
        if i < ln - 2:
            mensaje += ', '
    return mensaje

start = 5
end = 20
l = len(mensaje)

d = dict()
for i in range(start, end):
    for k in range(l - i):
        aux = mensaje[k:k + i]
        if aux not in d:
            d[aux] = [k]
        else:
            d[aux].append(k)

for (k, v,) in d.items():
    if len(k) % 5 == 0 and len(v) > 3:
        print('secuencia: {}, longitud: {}, posicion: {}, distancia: {}, factores:'.format(
            k, len(k), ','.join(map(str, v)), ourrenciascadenas(v)))

```

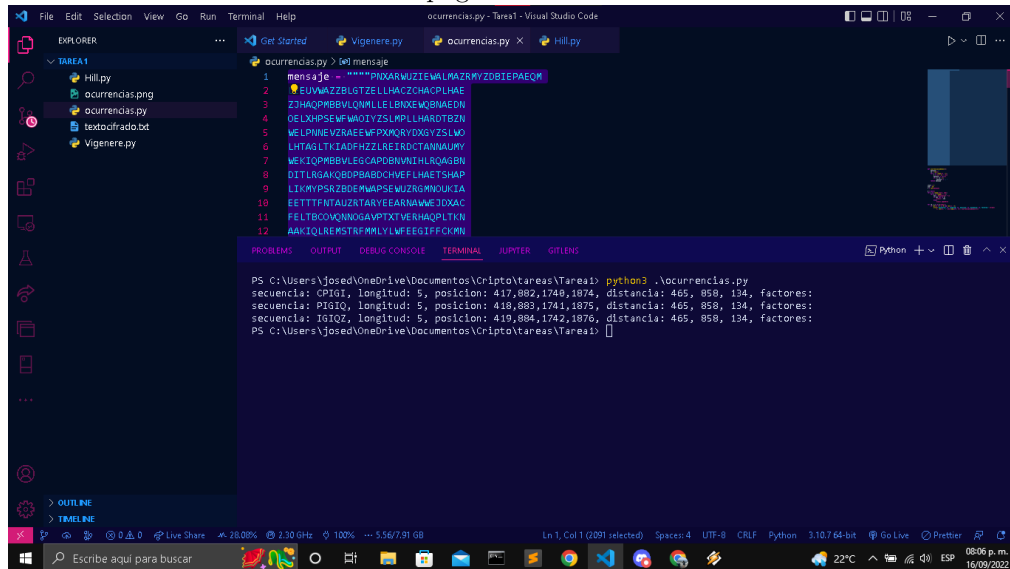
Al hacer el analisis de las ocurrencias repetidas en las cadenas los resultados fueron los siguientes:

Como se puede observar esas son las cadenas que mas se repiten y se puede observar que estas son de longitud 5 asi que con esto ya tenemos una aproximacion de que la clave para decifrar el texto de de 5 caracteres.

Ahora lo que sigue es sacar la tabla de frecuencias de este texto, para esto utilizaremos el codigo utilizado en el ejercicio 1 para las frecuencias. Al ejecutarlo con este texto obtuvimos los siguientes resultados:

Analizando con profundidad estos resultados me di cuenta que la llave de

ocurrencias.png ocurrencias.bb



```

1 mensaje = ****PHKARWUZIEMALMAZMYZOBIEPAEQM
2 EUNWAZZBLGTZELLHACZCHACPLHAE
3 Z3HACPMBBVLONMLLELBKXEWQBNADN
4 DELXHPSEFWMOIVZSLMPLHARDTEZN
5 WELPMNEVZRAEEWFPXMRVXGYZSLWO
6 LHTAGLTKIADPHZZLREIRDCTANNAUMY
7 WEIQPMBBVLEGCAPDENVAHLRQASBN
8 DITLRGAYGQOPHADOCHFFLAHETSHAP
9 LIKMYPSRZBDEWMADEWUZRGWMOUKIA
10 EETTTFTAUZATARVEEARNNAWJXAC
11 FELTBOOVNNOGAVPTXTVERHAQPLTKN
12 AAKIQLREWSTKFMMLYLWEEGIFPKMN

PS C:\Users\josed\OneDrive\Documents\Cripto\tareas\Tarea1> python3 .\ocurrencias.py
secuencia: CPIGI, longitud: 5, posicion: 417,892,1748,1874, distancia: 465, 858, 134, factores:
secuencia: PIIGI, longitud: 5, posicion: 418,883,1741,1875, distancia: 465, 858, 134, factores:
secuencia: IGIOZ, longitud: 5, posicion: 419,884,1742,1876, distancia: 465, 858, 134, factores:
PS C:\Users\josed\OneDrive\Documents\Cripto\tareas\Tarea1>

```

Figure 2: Resultado en consola al ejecutar el script anterior

desifrado es la palabra "LATIN". Ahora para hacer la decodificacion utilizaremos el siguiente programa para realizar la decodificacion de vigenere:

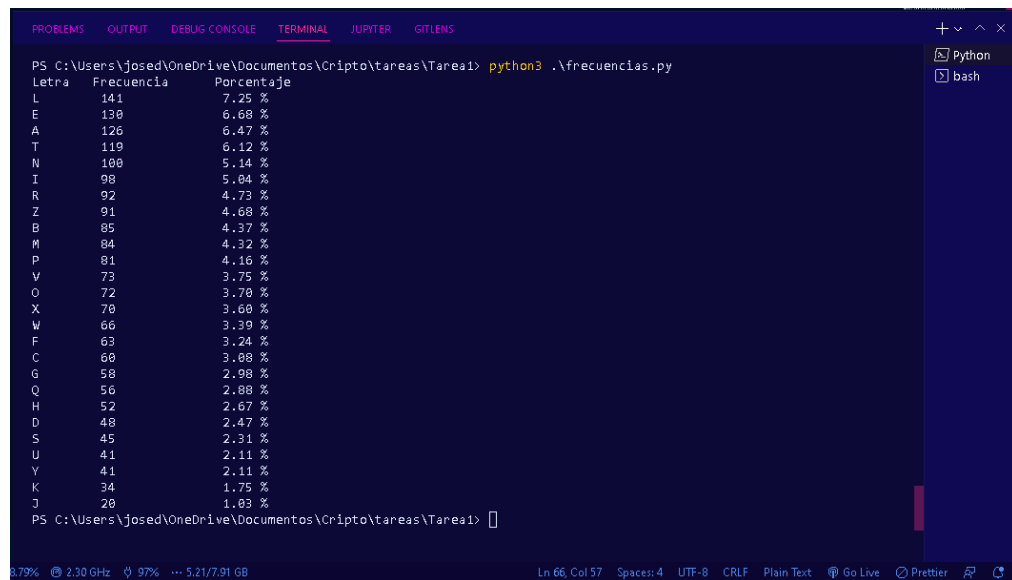
```

clave='LATIN'

def crackeaVinegere(x, k):
    ind1 = ord(x)-65
    ind2 = ord(k)-65
    return (ind1-ind2)%26

def desencripta(archivo):
    file = open(archivo,'r')
    texto = file.readlines()
    r = ''
    i = 0
    for line in texto:
        for char in line:
            if char.isalpha():
                c = clave[i%len(clave)]
                r = chr(crackeaVinegere(char, c)+65)
                print(r, end='')
                i += 1
            else:

```



```
PS C:\Users\josed\OneDrive\Documentos\Cripto\tareas\Tarea1> python3 .\frecuencias.py
Letra Frecuencia Porcentaje
L      141      7.25 %
E      130      6.68 %
A      126      6.47 %
T      119      6.12 %
N      100      5.14 %
I       98      5.04 %
R       92      4.73 %
Z       91      4.68 %
B       85      4.37 %
M       84      4.32 %
P       81      4.16 %
V       73      3.75 %
O       72      3.70 %
X       70      3.60 %
W       66      3.39 %
F       63      3.24 %
C       60      3.08 %
G       58      2.98 %
Q       56      2.88 %
H       52      2.67 %
D       48      2.47 %
S       45      2.31 %
U       41      2.11 %
Y       41      2.11 %
K       34      1.75 %
J       20      1.03 %
PS C:\Users\josed\OneDrive\Documentos\Cripto\tareas\Tarea1>
```

Figure 3: Resultado en consola al ejecutar el script anterior

```
print(char, end='')
```

```
desencripta('archivo.txt')
```

y nos deja el siguiente resultado en la terminal:\\

Por lo que el mensaje desifrado seria el siguiente:

```
EN ESE LUGAR LA  SENORA  ELODIA  REALIZA EL  MILAGRO AGARRA LOS POCOS PELOS
ROJOS DE  MI TIA QUE YA ESTA MEDIO CALVA
DESPUES LOS LAVA LOS SECA  LOS  ESTIRA
LES HACE CREPE  LOS  EXTIENDE Y  LOS  SOBA
HASTA  TRANSFORMAR LA ESCASA CABELLERA
DE  MI TIA EN UN  EDIFICIO D E FANTASIA DE
VARIOS PISOS CON RULOS  RISOS CAIRELES Y
ROSETON  ES LO HORNEA DURANTE
ALGUNAS  HORAS EN EL  SECADOR Y  DESPUES LO ROCIA
CON SIETE  LITROS  DE LACA PARA DARLE
FIRMEZA Y SOSTEN A  SU CREACION
EL DIA  DE LA BODA MI TIA LLEGO  A NUESTRA CASA  CON  UN PEINADO
QUE  MEDIA DOS METROS DE ALTURA SE  VEIA IMPRESIONANTE CUANDO
ABRIMOS  LA PUERTA PARA
SALIR SE ESCUCHO UN ZUMBIDO AL  LEVANTAR LA VISTA AL  CIELO  DESCUBRIMOS UN
BICHO QUE SE ACERCABA  VOLANDO A TODA
```

```
PS C:\Users\josed\OneDrive\Documentos\Cripto\tareas\Tarea1> python3 .\VigenereDesifrado.py
E NE SEL UGA RLA SEN ORA ELO DIA REA LIZ
AEL MIL AGR OAG ARR ALO SPO COS PELOS R
OOO SDE MIT IAQ UEY AES TAM EDI OCA LVA

DES PUE SLO SLA VAL OSS ECA LOS EST IRA
LES HAC ECR EPE LOS EXT IEN DEY LOS SOB
AHA STA TRA NSF ORM ARL AES CAS ACA BEL
LER ADE MIT IAE NUN EDI FIC IOD EFA NTA
SIA DEV ARI OSP ISO SCO NRU LOS RIS OSC
ATR ELE SYR OSE TON ESL OHO RNE ADU RAN
TEA LGU NAS HOR ASE NEL SEC ADO RYD ESP
UES LOR OCI ACO NSI ETE LIT ROS DEL ACA
PAR ADA RLE FIR MEZ AYS OST ENA SUC REA
CIO NEL DIA DEL ABO DAM ITI ALL EGO ANU
EST RAC ASA CON UNP EIN ADO QUE MED IAD
OSM ETR OSD EAL TUR ASE VEI AIM PRE SIO
NAN TEC UAN DOA BRI MOS LAP UER TAPARA
SAL IRS EES CUC HOUNZU MBI DOA LLEVAN
TAR LAV IST AAL CIE LOD ESC UBR IMOS UN
BIC HOQ UES EAC ERC ABA VOL AND OATODA
VEL OCI DAD QUE ESE SOP REG UNT OMIMAM
AYO SEL OQU EES ACLARE TRIUNFAL CUAN
DOL OPU DED IST ING UIR MAS DEC ERCAES
UNM AYA TEY ESO QUE ESI NTE RRO GOMIHE
RMA NAU NMA YAT ELE SIN FOR MEE SUNAES
PEC IED EES CAR ABA JOP ERO UNP OCOMAS
REC HON CHO ELM AYA TEE RAD ELM ISMO CO
LOR ROJ OBR ILL ANT EQU EEL CAB ELLO DE
MIT IAE LIN SEC TOV OLO ENP ICA DAYZAO
SEZ A MB ULL OEN ELP EIN ADO AYQ UEASCO
GRIT OM IMA MAA YQU ESU STO BER REOMIH
ERM A NA AYQ UEB ARB ARI DAD SEH ISTERI
ZOM ITI AQU ITE NME LOP ERO SIN DESCOM
PON ERE LPE INA DOA DVI RTI ONO SASOMA
MOS TEM ERO SOS ALA SPR OFU NDI DADESD
EES A SE LVA ROJ AYA LOV IDI JOM IPAPAE
```

Figure 4: Resultado en consola al ejecutar el script anterior

VELOCIDAD QUE ES ESO PREGUNTO MI MAMA
YO SE LO QUE ES ACLARE TRIUNFAL CUANDO LO PUDE DISTINGUIR MAS DE CERCA ES
UN MAYATE Y ESO QUE ES INTERROGO MI HERMANA UN MAYATE LES INFORME
ES UNA ESPECIE DE ESCARABAJO PERO UN POCO MAS
RECHONCHO EL MAYATE ERA DEL MISMO COLOR ROJO BRILLANTE
QUE EL CABELLO DE
MI TIA EL INSECTO VOLO EN PICADA Y ZAO
SE ZAMBULLO EN EL PEINADO AY QUE ASCO
GRITO MI MAMA AY QUE SUSTO BERREO MI HERMANA
AY QUE BARBARIDAD SE HISTERIZO MI TIA QUITENMELO PERO SIN
DESCOMPONER EL PEINADO ADVIRTIO NOS ASOMAMOS TEMEROSOS A LAS PROFUNDIDADES
DE ESA SELVA ROJA YA LO VI DIJO MI PAPA ESTA UN POCO ATURDIDO Y MAREADO POR EL
OLOR DE LA LACA SAL DE AHI EL MAYATE NO OBEDECIO LE METIMOS
UN LAPIZ HURGAMOS
CON EL DEDO LE SOPLAMOS Y NADA EL PEINADO SEGUIA INTACTO ADENTRO DE NADA
VALIERON SUPlicas AMENAZAS NI LOS MAS RUDOS PROCEDIMIENTOS NI MODO SE
IMPACIENTO MI PAPA SE NOS HACE TARDE
TENDRAS QUE IR CON ESO MI TIA AUNQUE NERVIOSA
SABIA QUE NO TENIA OTRA ALTERNATIVA LA FIESTA TRANSCURRIA NORMALMENTE
PERO MI TIA SE SOBRsaltaba A CADA RATO CUANDO TERMINAMOS DE CENAR
Y EMPEZO LA MUSICA MI TIA AHOGO UN GRITO QUE TE PASA LE PREGUNTE CREO QUE
EL ESCARABAJO ESTA BAILANDO SUSURRO ME ASOME AL PEINADO Y EFECTIVAMENTE

Figure 5: Resultado en consola al ejecutar el script anterior

EL ESCARABAJO ROJO ESTABA BAILANDO EL PRIMER VALS DE LA NOCHE OBSERVE
FASCINADO QUE EL MERENGUE DEL PASTEL
DE BODAS TENIA GRANDES SEMEJANZAS CON
EL PEINADO DE MI TIA LLEGO EL MOMENTO
DE FELICITAR A LOS NOVIOS MI TIA SE
LEVANTO COMO TODOS Y AL ABRAZAR A LA NOVIA ZZ EL ESCARABAJO DECIDIO VOLAR
EN EL INTERIOR DEL PEINADO QUE ES ESE RUIDO PREGUNTO LA NOVIA ALGO ASUSTADA
PARECE QUE VIENE DE TU CABEZA TIA ES
MI APARATO PARA LA SORDERA RESPONDIO
ELLA CON UNA SONRISA DE PANICO

5 Problema 5

El siguiente mensaje fue cifrado con el algoritmo de Hill poniendo en correspondencia $a=0, \dots, z=25$, sin ñ, ni puntos ortográficos

- Encuentre la matriz de cifrado y proporcione solo las ecuaciones que lo llevan al resultado.
- Encuentre la matriz de descifrado.
- Descifre el mensaje.

Partiendo de que se tiene la siguiente correspondencia PP EK TC DW DS
YA WE MI NA RS FG proviene de "El sabado fuimos a una boda".

PP EK TC DW DS YA WE MI NA RS FG CK JD IM MA GQ XM EH QC RS FG ND DH GC
EW HK WG BE BI TI LV ME OF NN RO LI OF VT FZ UG LT WQ UM YI QH MA BW WW
WG SW RH EU WW TO FP UO TP QL SY QC JC PP OK JC FR LI IE WU NN PY ND DH FX
EU RH IC EO OK OC DR DU MK EO XV RH QC DU ND BP WG UG DC ZH IG NA DW GI
AQ QO UJ FX EU DB LD NL JT VG MK LI KU GG XY TP EO JD EQ JR DB DH RH EW HK
WG BE BI DO EQ DB WG XV SM FM RY RH TP XS LO SD NF SM ZM PE