Universidad Nacional Autónoma de México

Facultad de Ciencias

Criptografía y Seguridad

Tarea 1

Cifrados Clásicos

Profesor:

Manuel Díaz Díaz

Integrantes:

Lázaro Pérez David Jonathan

Licona Gómez Aldo Daniel

Marín Parra José Guadalupe de Jesús

1. Explique brevemente porque en $\mathbb{Z}_n$ dados $a \cong bmod(n)$ y $c \cong dmod(n)$, se tiene que $ac \cong bdmod(n)$.
RESPUESTA.
Porque si tenemos $a \cong bmod(n)$ y $c \cong dmod(n)$ sabemos que $a - n$ y $c - d$ son divisibles entre n, por lo que $(a + c) - (b + d) = (a - b) + (c - d)$ es divisible entre n, así que $a + c \cong b + dmod(n)$. Además $(a - b)c$ es divisible entre n y $b(c - d)$ que es divisible entre n, por lo tanto $ac - bd = (a - b)c - b(c - d)$ que es divisible entre n, así $ac \cong bdmod(n)$.

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

$$\begin{aligned} x &\cong 25mod(35) \quad (1)\\ x &\cong 15mod(65) \quad (2)\\ x &\cong 10mod(15) \quad (3)\\ x &\cong 35mod(55) \quad (4)\\ x &\cong 55mod(85) \quad (5) \end{aligned}$$

RESPUESTA.
Analizando las soluciones.
Para (1) y (2) tenemos que $(n_1, n_2) = (35, 65) = 5$ y $a_2 - a_1 = 25 - 15 = 10$. Como 5 divide a 10 entonces hay solución con (1) y (2).

Para (1) y (3) tenemos que $(n_1, n_3) = (35, 15) = 5$ y $a_3 - a_1 = 25 - 10 = 15$. Como 5 divide a 15 entonces hay solución con (1) y (3).

Para (1) y (4) tenemos que $(n_1, n_4) = (35, 55) = 5$ y $a_4 - a_1 = 35 - 25 = 10$. Como 5 divide a 10 entonces hay solución con (1) y (4).

Para (1) y (5) tenemos que $(n_1, n_5) = (35, 85) = 5$ y $a_5 - a_1 = 55 - 25 = 30$. Como 5 divide a 30 entonces hay solución con (1) y (5).

Para (2) y (3) tenemos que $(n_2, n_3) = (65, 15) = 5$ y $a_3 - a_2 = 15 - 10 = 5$. Como 5 divide a 5 entonces hay solución con (2) y (3).

Para (2) y (4) tenemos que $(n_2, n_4) = (65, 55) = 5$ y $a_4 - a_2 = 35 - 15 = 20$. Como 5 divide a 20 entonces hay solución con (2) y (4).

Para (2) y (5) tenemos que $(n_2, n_5) = (65, 85) = 5$ y $a_5 - a_2 = 55 - 15 = 40$. Como 5 divide a 40 entonces hay solución con (2) y (5).

Para (3) y (4) tenemos que $(n_3, n_4) = (15, 55) = 5$ y $a_4 - a_3 = 30 - 15 = 20$. Como 5 divide a 20 entonces hay solución con (3) y (4).

Para (3) y (5) tenemos que $(n_3, n_5) = (15, 85) = 5$ y $a_5 - a_3 = 55 - 15 = 40$. Como 5 divide a 40 entonces hay solución con (3) y (5).

Para (4) y (5) tenemos que $(n_4, n_5) = (55, 85) = 5$ y $a_5 - a_4 = 50 - 35 = 20$. Como 5 divide a 20 entonces hay solución con (4) y (5).

El sistema tiene solución, por lo qeu se solucionará en primera instancia (1) y (2).

$x \cong 25 mod(35)$ (1)
$x \cong 15 mod(65)$ (2)

Si $x \cong 25 mod(35)$, entonces $x = 25 + 35k_1$ con k_1 en $\mathbb{Z}$, como x también es solución de (2) entonces tenemos $25 + 35k_1 \cong 15 mod(65)$, lo que equivale a que $35k_1 \cong 25 - 15 mod(65)$, lo que es lo mismo que $35k_1 \cong 10 mod(65)$. Haciendo la división correspondiente tenemos $7k_1 \cong 2 mod(13)$ con lo que tenemos que $x = 25 + 35(k_1) = 25 + 35(9) = 25 = 315 = 340$. Al final obtenemos $x \cong 340 mod(455)$ (1.1)

Para (3) y (4).
$x \cong 10 mod(15)$ (3)
$x \cong 35 mod(55)$ (4)

Si $x \cong 10 mod(15)$, entonces $x = 10 + 15k_2$ con k_2 en $\mathbb{Z}$, como x también es solución de (4) entonces tenemos $10 + 15k_2 \cong 35 mod(55)$, lo que equivale a $15k_2 \cong 35 - 10 mod(55)$ que es $15k_2 \cong 25 mod(55)$. Haciendo la división correspondiente tenemos $3k_2 \cong 5 mod(11)$ con lo que tenemos que $x = 10 + 15(k_2) = 10 + 15(9) = 10 + 135 = 145$. Al final obtenemos $x \cong 145 mod(165)$ (1.2)

Para (1.1) y (1.2)
$x \cong 340 mod(455)$ (1.1)
$x \cong 145 mod(165)$ (1.2)

Si $x \cong 340 mod(455)$, entonces $x = 340 + 455k_3$ con k_3 en $\mathbb{Z}$, sustituyendo tenemos $340 + 455(k_3) \cong 145 mod(165)$, es decir, $455k_3 \cong 195 mod(165)$ equivalente a $91k_3 \cong 39 mod(33)$ con lo que se tiene $x = 240 + 455(9) = 340 + 4095 = 4435$. Al final obtenemos $x \cong 4435 mod(15015)$ (1.1.1)

Por último para (1.1.1) y (5)
$x \cong 4435 mod(15015)$ (1.1.1)
$x \cong 55 mod(85)$ (5)

Si $x \cong 4435 mod(15015)$, entonces $x = 4435 + 15015k_4$ con k_4 en $\mathbb{Z}$, sustituyendo tenemos $4435 + 15015(k_4) \cong 55 mod(85)$, es decir, $15015k_4 \cong 4380 mod(85)$ rquivalente a $3003k_4 \cong 876 mod(17)$ con lo que se tiene $x = 4435 + 15015(10) = 4435 = 150150 = 154585$.

Al final cualquier solución es congruente con $x \cong 154585 mod(255255)$.

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

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 RXTPFKQRSLQ NPRQFMKRQ QRIRSTFVLQ QF KM TLJAFRK L IL SLNLSFELE JUTLSFMKLI FKDRPKRTR ERI VFPUQ. LOUF LNIFSLJMQ UKL NPURAL ER RVMIUSFMK ER QUQTFTUSFMK

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 LSREMQ. IMQ LJFKMLSFEMQ SMJNLPTFEM RKTPR TMELQ ILQ NPMTRFKLQ Q OUR QR UKRK L LSREMQ NRPJLKRSRK SMKQTLKTRQ IM OUR FKEFSL OUR RQTMQ LJFKMLSFEMQ QMK RQRKSFLIRQ NLPL IL UKFMK NPRSFQL LI PRSRNTMP. IMQ SMJNIRGMQ PAE NLPL SLEL VLPFLTR SMK RI PRSRNTMP QR UTFIFZLPMK NLP FERKTFBFSLP IMQ LJFKMLSFEMQ FKVMIUSPLEMQ RK IL FKTRPLSSFMK NPMTRFKL NPMTRFKL. IL PAE ER MJFSPMK RQTLAIRSR MSDRKTL Y EMQ SMKTLSTMQ BPRKTR L IMQ QRQRKTLYSULTPM ER IL NPMTRFKL MPFCFKLI ER WUDLK NMP IM TLKTM, RI KUJRPM 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 RQTPUSTUPL 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 EFBRPRKTR ER IL NPMTRFKL MPFCFKLI OUR NPMVMSLK UK PRSMKMSFJFRKTM PREUSFEM NMP NLPTR ER IMQ LKTFSURPNMQ KRUTPLIFZLKTRQ. KURQTPMQ PRQUITLEMQ QUCUFRPRK OUR ILQ NPRQFMKRQ QRIRSTFVLQ QMK FKEUSFELQ NMP ILVLSUKLSFMK JLQFVL RK TMEM RI JUKEM Y NMP NRPQFQTRKSFL ER FKBRSSFMRQ PRSUPPRKTRQ RK FKEFVFEUMQ FKJUKMERNPFJFEMQ, OUR KM RIFJFKLPMK IL FKBRSSFMK Y LSLALPMK BLSFIFTLKEM IL QRIRSSFMK ER VFPUQ SUYLQ SLPLSTRPFQTFSLQ QMK EFBRPRKTRQ L IMQ SMV LKTRPFMPRQ, JRKMQ NLTMCRKMQ NRPM SMK JLYMP TPLKJFQFAFIFELE.

RESPUESTA.

Dado que el mensaje es en el lenguaje español, no hay acentos ni ñ y conservamos la separación de palabras según el mensaje original, entonces veamos la tabla de frecuencias del mensaje anterior la cual es la siguiente.

Letra	Frec.	%	Letra	Frec.	%
R	210	10.12	J	46	2.22
L	200	9.63	V	24	1.16
M	172	8.29	Y	14	0.67
Q	142	6.84	A	14	0.67
K	141	6.79	C	11	0.53
F	132	6.36	B	9	0.43
P	117	5.64	O	8	0.39
S	108	5.2	D	7	0.34
T	92	4.43	G	3	0.14
E	90	4.34	Z	3	0.14
I	88	4.24	H	1	0.05
U	60	2.89	X	1	0.05
N	56	2.7	W	1	0.05

Tabla de frecuencias caracteres en el texto cifrado.

Si observamos el texto cifrado podemos notar que la letra L tiene muchas apariciones, muchas de ella son solo la letra L, es decir, podemos afirman que L es una vocal o es 'y'. Sin embargo también observamos gracias a nuestra tabla de frecuencias que Y se repite varias veces y si

vamos al texto cifrado, notamos que Y siempre aparece sola, por lo que $\underline{Y = \text{'}y\text{'}}$, entoces L es cualquier vocal.

Notamos en el texto cifrado que hay apariciones de palabras con dos letras como IL, ER, DL, QR y demás. Por ahora nos centramos en IL ya que contiene a la L, entonces I debe ser consonante, como IL y L tienen bastantes apariciones en el texto entonces $\underline{L = \text{'}a\text{'}}$ ya que es una vocal muy común en el idioma español. También notamos que existe la palabra ERI en el texto, como IL tiene a 'a' e IL aparece constantemente entonces $\underline{I = \text{'}l\text{'}}$, entonces decimos que la palabra ERI termina en l, lo cual en español es un conector, se trata de del, dicho esto tenemos que $\underline{E = \text{'}d\text{'}}$ y $\underline{R = \text{'}e\text{'}}$.

Por ahora solo hemos descubierto 5 letras de nuestro alfabeto.

Analicemos el primer párrafo del texto cifrado con las letras que ya tenemos. Sustituimos las letras que ya desciframos y tenemos los siguiente.
la NPMTeFKa QNFHe del QaPQSMVdMQ Qe eQTa adaNTaKdM deAFdM a NPeQFMKeQ
IL NPMTRFKL QNFHR ERI QLPQSMVEMQ QR RQTL LELNTLKEM ERAFEM L NPRQFMKRQ

QeleSTFVaQ
QRIRSTFVLQ

Observamos que tenemos Qe y $eQTa$, esta última se parece mucho a la palabra 'esta', entonces $\underline{Q = \text{'}s\text{'}}$ y $\underline{T = \text{'}t\text{'}}$. Volvamos a sustituir el primer párrafo con nuestras dos nuevas letras.

la NPMteFKa sNFHe del saPsSMVdMs se esta adaNtaKdM deAFdM a NPesFMKes
IL NPMTRFKL QNFHR ERI QLPQSMVEMQ QR RQTL LELNTLKEM ERAFEM L NPRQFMKRQ

seleStFVas
QRIRSTFVLQ

Por segunda ocasión notamos que $seleStFVas$ se parece a la palabra 'selectivas' por lo que $\underline{S = \text{'}c\text{'}}$, $\underline{F = \text{'}i\text{'}}$ y $\underline{V = \text{'}v\text{'}}$. Sustituimos nuevamente en el primer párrafo.

la NPMteiKa sNiHe del saPscMvdMs se esta adaNtaKdM deAidM a NPesiMKes
IL NPMTRFKL QNFHR ERI QLPQSMVEMQ QR RQTL LELNTLKEM ERAFEM L NPRQFMKRQ

selectivas
QRIRSTFVLQ

Ahora ya no es tan claro ver más similitudes con es español, tómemos un fragmento del segundo párrafo para encontrar más letras.

la escala CIMAal de la NaKdeJia de cMvid Da deJMstPadM la evMlUciMK
IL RQSLIL CIMALI ER IL NLKERJFL ER SMVFE DL ERJMQTPLEM IL RVMIUSFMK

del saPQcMvdMQ
ERI QLPQSMVEMQ

Notamos que $cMvid$ se parece a 'covid' por lo que $\underline{M = \text{'}o\text{'}}$ y también que $deJostPado$ es 'demostrado' y $evolUcio$ es 'evolución'. Entonces tenemos que $\underline{J = \text{'}m\text{'}}$, $\underline{P = \text{'}r\text{'}}$ y $\underline{U = \text{'}u\text{'}}$.

Volvamos la primer párrafo y sustituyamos.

la NroteiKa sNiHe del sarscovdos se esta adaNtaKdo deAido a NresioKes
IL NPMTRFKL QNFHR ERI QLPQSMVEMQ QR RQTL LELNTLKEM ERAFEM L NPRQFMKRQ

selectivas
QRIRSTFVLQ

Entonces tenemos que $NresioKes$ es 'presiones', $adaNtaKdo$ es 'adaptando' y $deAido$ es debido por lo que $N =$'p', $K =$'n' y $A =$'b'. Sustituyamos.

la proteina spiHe del sarscovdos se esta adaptando debido a presiones
IL NPMTRFKL QNFHR ERI QLPQSMVEMQ QR RQTL LELNTLKEM ERAFEM L NPRQFMKRQ

selectivas
QRIRSTFVLQ

Entonces $H =$'k' de tal forma que el primer párrafo queda como sigue.

'la proteina spike del sarscovdos se esta adaptando debido a presiones selectivas'

Hagamos nuestra tabla de asociación.

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

Tabla de asociación.

Como aún no tenemos el alfabeto completo, entones tomaremos palabras con las letras aún sin descifrar y las descifraremos.

Tenemos la palabra 'DLK', sustituyendo queda 'Dan' y por el tamaño de la cadena podemos decir que es un conector y que 'DLK' es 'han', entonces $D =$'h'.

También tenemos 'CIMALI' que es 'Clobal' y es 'global' por lo que $C =$'g'.

Como no hay muchas apariciones de W, X y Z suponemos que no cambian su valor en el alfabeto, de tal forma que la tabla va quedando de la siguiente manera.

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

Tabla de asociación.

Ahora sólo tenemos que averiguar f, j y q y las últimas candidatas son B, G y O. Como son las últimas solamente las asociamos y tenemos nuestra tabla completa.

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

Tabla de asociación.

Entonces el alfabeto clave para descifrar el mensaje es LASERBCDFGHIJKMNOPQTUVWXYZ.

Y el mensaje descifrado es el siguiente.

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 INHERNETE 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 VARIENTE 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 VARIATE CON EL RECEPTOR SE UTILIZARON PAR 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 ARMSD, CAUSADO POR UN CONJUNTO DE MUTACIONES CERCANAS A LA GLICOSILACION NTRESITNEO 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 SUGUIEREN QUE LAS PRESIONES SELECTIVAS SON INDUCIDAS POR LAVACUNACION MASIVA EN TODO EL MUNDO Y POR PERSISTENCIA DE INFECCIOES RECURRENTES EN INDIVIDUOS INMUNODEPRIMIDOS, QUE NO ELIMINARON LA INFECCION Y ACABARON FACILITANDO LA SELECCION DE VIRUS CUYAS CARACTERISTICAS SON DIFERENTES A LOS COV ANTERIORES, MENOS PATOGENOS PERO CON MAYOR TRANMISIBILIDAD.

4. El siguiente cifrado es implementado en Vigenere, los caracteres fueron puestos en una biyección del 0 al 25 donde $a = 0$ y $25 = z$ sin signos de puntuación ni ñ.

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 ZJH 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

2

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 ZNX 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 Z 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

Aplique la prueba de Kaisiski de la longitud de la clave, la clave y después descifre el mensaje.
RESPUESTA.

El mensaje está dividido en bloques de tres.

Secuencia	Frecuencia	Posiciones	Distancias	Factores
LE	5	30, 70, 190, 1165, 1293	45, 115, 975, 128	$3 \cdot 3 \cdot 5, 5 \cdot 23, 3 \cdot 5 \cdot 5 \cdot 13,$ $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$
ZZ	8	37, 163, 1124, 1139, 1254, 1378, 1662, 1749	126, 961, 15, 115, 124 284, 87	$2 \cdot 3 \cdot 3 \cdot 7, 31 \cdot 31, 3 \cdot 5, 5 \cdot 23,$ $2 \cdot 2 \cdot 31, 2 \cdot 2 \cdot 71, 3 \cdot 29$
LL	12	45, 74, 110, 427, 430, 520 664, 699, 1104, 1380, 1600, 1602	29, 36, 317, 3, 90, 144, 35, 405, 276, 220, 2	29, 2 · 2 · 3 · 3, 317, 3, 2 · 3 · 3 · 5, 2.2.2.2.3.3,5.7,3.3.3.3.5, $2 \cdot 2 \cdot 3 \cdot 23, 2 \cdot 2 \cdot 5 \cdot 11, 2$
PL	18	55, 109, 239, 325, 370, 554, 729, 815, 965, 1025, 1085, 1100, 1145, 1214, 1500, 1504, 1715, 1879	54, 130, 86, 45, 184, 175, 86, 150, 60, 60, 15, 45, 69, 286, 4, 211, 164	$2 \cdot 3 \cdot 3 \cdot 3, 2 \cdot 5 \cdot 13, 2 \cdot 43,$ $3 \cdot 3 \cdot 5, 2 \cdot 2 \cdot 2 \cdot 23, 5 \cdot 5 \cdot 7,$ $2 \cdot 43, 2 \cdot 3 \cdot 5 \cdot 5, 2 \cdot 2 \cdot 3 \cdot 5,$ $2 \cdot 2 \cdot 3 \cdot 5, 3 \cdot 5, 3 \cdot 3 \cdot 5, 3 \cdot 23$ $, 2 \cdot 11 \cdot 13, 2 \cdot 2, 211,$ $2 \cdot 2 \cdot 41$
AE	19	26, 58, 86, 130, 233, 269, 381, 481, 509, 720, 1346, 1356, 1384, 1445, 1540, 1709, 1744, 1766, 1839	32, 28, 44, 103, 36, 112, 100, 28, 211, 626, 10, 28, 61, 95, 169, 35, 22, 73	2.2.2.2.2, 2.2.7, 2.2.11, 103, 2.2.3.3, 2.2.2.2.7, 2.2.5.5, 2.2.7, 211, 2.313, 2.5, 2.2.7, 61, 5.19, 13.13, 5.7, 2.11,73
BB	7	67, 187, 544, 593, 872, 1268, 1392	120, 357, 49, 279, 396, 124	2.2.2.3.5, 3.7.17, 7.7, 3.3.31, 2.2.3.3.11,2.2.31
NN	10	124, 174, 309, 359, 394, 401, 623, 1089, 1184, 1924	50, 135, 50, 35, 7 222, 466, 95, 740	2.5.5,3.3.3.5,2.5.5,5.7, 7,2.3.37,2.233,5.19,2.2.5.37
LR	18	165, 203, 213, 335, 428, 615, 730, 808, 915, 1113, 1288, 1440, 1505, 1603, 1788, 1900, 1908, 1938	38, 10, 122, 93, 187, 115, 78, 107, 198, 175, 152, 65, 98, 185, 112, 8, 30	2.19,2.5,2.61,3.31,11.17, 5.23,2.3.13,107,2.3.3.11 ,5.5.7,2.2.2.19,5.13,2.7.7 ,5.37,2.2.2.2.7,2.2.2,2.3.5
EE	17	131, 270, 286, 350, 571, 765, 771, 940, 1166, 1290, 1385, 1425, 1561, 1591, 1631, 1776, 19211	139, 16, 64, 221, 194, 6, 169, 226, 124, 95, 40, 136 136, 30, 40, 145, 145	139,2.2.2.2,2.2.2.2.2.2, 13.17,2.97,2.3,13.13,2.113, 2.2.31,5.19,2.2.2.5,2.2.2.17, 2.3.5,2.2.2.5,5.29,5.29
TT	10	273, 1002, 1051, 1087, 1202, 1406, 1482, 1697, 1757, 1902	729, 49, 36, 115, 204, 76, 215, 60, 145	3.3.3.3.3.3,7.7,2.2.3.3,5.23, 2.2.3.17,2.2.19,5.43,2.2.3.5, 5.29
WW	4	292, 972, 1522, 1832	680, 550, 310	2.2.2.5.17,2.5.5.11
MM	5	343, 1337, 1477, 1647, 1657	994, 140, 170, 10	2.7.71,2.2.5.7,2.5.17,2.5
AA	5	330, 829, 1045, 1054, 1940	499, 216, 9, 886	499, 2.2.2.3.3.3,3.3,2.443
RR	4	384, 589, 870, 1441	205, 281, 571	5.41, 281, 571
CC	3	444, 655, 1834	211, 1179	211,3.3.131

Como podemos ver los Factores que mas se repiten son 2,3 y 5, ahora bien la clave no puede ser tan pequeña como para considerar que es de tmaño 2 o 3 por lo que tomamos al 5 como tamaño de la clave.

Ahora dividimos el texto en columnas de 5 y colocamos la respectiva letra en cada una como sigue

lista1:
P W W Z Z P L W L L Z P Z P L L X N O P W Z L D W N A P Y Z L L D L D N W P L
P N Q D G D D F T L P D P Z O E F Z Y N J F C N P E P A L T L E F N W P O T R
P N Z P Z P Z C L L T C Y N Z X A L D D F Y T W E G L W N X M B L L W L G T
F D R X L W P L T W O F D F D C F L D P P Z C F L D C F A O L U Z N C Y W E
O D W U W P W W X P P Z A L D M P P Z P R X L P Z P P L P L O D K T E W Z P
A P Y O T L X X Z D F L P P Z W T A D A E O C A Z P N O P L Z N X Z L F Z P Z
A D L T D L N P O L P F L Y Y X O Z X Z Z T T X L D E E L T P E Y P D T Y T L
C G T E N L L E Z L M W L C F E Y O L A L N T R C F L A Y P P L U L L F Z Z A
O P L P N L U L T Z T L W S P L L P C P L O L T Y P Y Z P Z E P X E P E Z T E
W E Z D M C Z K N L N G P Y C P Z D F C E Z W F L N G O L E X C L D C A Z N L T A Z

lista2:
N U A R D A E A G L C L J M Q E E A E S A S L T E E E X D S H T F R C A E M
E D I A I A P C L S I S E S R U E N R E A D E O O T R L A R R Y E C I D L A A
O S A N I Q D S O L S A E A U A O U P A E C Z D E A I L O U O I U C B A T E D
E O U I Y O S R U C O D T I D C N T O S R M M N T I M N E E R O U O E C M
E E M O O L Q C L I L C L I Y E U N I A A R I A S B O R A B R S T O A E O S S
O L A V O S O E S P N D E L J O J A T O U O E O L L A E L T B I E S P R S L L
L Y E N E I T N E V R P S A I A O C I S D M E I S H A E S R S I Q R A A O A A
N A E R U N L E M S R T C A A E A E R E M A A O I E S R T O L R O B N S M
M E O C M E A J O B L E M L A E R S D E E D S E S A D M Z N I D I G O O L A
S O I E O T Y R A V E A J I O N E D I Q E I E O V G S P E I E B I I A R O A O E O S S A

lista3:
X Z L T B E E Z T H H H H H B N L W E L E O L H B L V E M X L T K H E T U K B G
B H G T K B H H H K R M E G K T T T E W X L V G X H T K E F L G K H B T F E T
M L N G N B F L M X B L G T U L X T E X A N H O K L V W U L V X X T G H E T
X I G F H J T X G N E X B K X T F X J B K B T F X G X T V X T I G F V A T X E H
K U T N T H M B M H V S S E X G R L B F R N X F F R T B X X F J G I B V G I W
B G H L K T K W X L O T O H I T V K R T K H T L T F X X H M N B Z V W X T G
E T Z G H M G T H E T S E L L X X G H I G I X T K G J V H T N O L J M H E T E L
T K H F I B X X T T M G K F V R S N F T N M M T X X J X T X T W N X X B R M
X E K H X T T E X L G H O V H E G X M U M Z X X T X G X T H F W B K G L T O
V H T T E B E K H W E X K X G N L W Z E B H M T J X M X T T M T K K G E G H T G

lista4
A I M M I Q U Z Z A A A A B M B Q D X W I M A Z P Z W Q G W A I Z I A M I B C
N L B L Q A V A A M Z W W M I T A A A W A T Q A T A K I M M W I M V I J Q T
V Z I V I M I M L C D U Q B V Z T Z Z Q A W U I I T B Q M Z C P A Z D L L W L
A Z B I A C K B N I W L V U K M I G C V W P V I T N M M Q A J M X I P W G Z
U K Z Z V M J L Q V W M I I I T T I Y K B I Y A Z Q I Y Z L P Z Q C U M V W M
M W Z W U B W T W Q A I I G Q U I C W L U L M Z T I P I V L T Q V H I W M A
U I X L C B I Z I T V Q U I W Z X L V Q A I B I V K L L C W U I M Q I C M B B B I
B V Z Z M M B A A J L W L U W M M W A Q P V W M T O K C A J A Q W Z I I V
M Q V M I Z A J V X Z L W J M Q Y U O T M W M Z A R A T I U T M M M K I W
U A I W L T H I I M I L Q I T Q T I M M W C I I I I Z C V C H M X W T L M L T C V L Q

lista5
R E A Y E M V B E C C E Q V L N B N H F Y P R N N R F R Y O G A Z R N Y Q V A
V R N R B B E E P Y B A U N A T U R R E C B N V V Q N Q S M F F N R Q B G R H
N P C Q Z Q G R E R C B R Q V N G N E P H O Y A N N R F V A B R P B B N P D R
R B Z R R Y E N A C V T N R F L R R G T R N L R B F F R P N E B F B R N N V B
B V G R R R N F I A Q B Z B C Q H B B Z H G E U A H O N V V G V R E Q Z E V N
G F N R F N S Q Q F E N Q V R A N V N B Y Q N Y V L B R R Z Y U Z A Q B B Q
R B V N Q B Q V F P R F F H E V G Z R P B C B R R E R A V H A B O R A E R V
S N F V Z A E V B N N N P B V F A Z Y V G B T D C R H E R P N G Y F E F Y N
S I G F O B G N Q E I R P F S A H R H C Y Q A N F N P C Q V Y Y A S V Y I V R
A Z B N N A M F O R B E V B C Q R E C A A N F Q R R R P N F N C N R F V N A E R P

Ahora contemos cuantas veces se repite una letra en la lista 1

Lista 1
A = 15
B = 1
C = 17
D = 26
E = 20
F = 19
G = 6
H = 0
I = 0
J = 1
K = 2
L = 63
M = 4
N = 21
O = 16
P = 53
Q = 1
R = 4
S = 1
T = 23
U = 4
V = 0
W = 23
X = 14
Y = 15
Z = 41

Como podemos ver el caracter que mas se repite es la letra L pero tambien esta muy cerca la letra P por lo que analizaremos cual nos conviene más.

La letra L con E nos da la letra T y la letra P con E nnos da la letra L, ahora la letra L que nos da P tiene una mayor frecuencia de uso por lo que tomaremos a la letra P como primer letra de la clave que nos da la letra L.

Ahora veamos la lista 2

Lista 2
A = 49
B = 7
C = 14
D = 17
E = 57
F = 1
G = 3
H = 2
I = 30
J = 5
K = 0
L = 25
M = 15
N = 15
O = 41
P = 6
Q = 5
R = 25
S = 34
T = 14
U = 12
V = 4
W = 0
X = 1
Y = 5
Z = 2

Como podemos ver la letra A Y E son las que más se repiten, de igual forma veamos cual nos conviene más, la letra E con la letra A nos da la letra W y la letra A con A nos dan la letra A y la letra A tiene una mayor frecuencia por lo que tomaremos a la segunda letra de la clave a A que nos da A.

Ahora veamos la lista 3

Lista 3
A = 2
B = 23
C = 0
D = 0
E = 28
F = 16
G = 31
H = 36
I = 8
J = 7
K = 24
L = 25
M = 18

N = 13
O = 7
P = 0
Q = 0
R = 7
S = 4
T = 56
U = 5
V = 14
W = 10
X = 49
Y = 0
Z = 6

Como podemos ver las letras T y X son las que mas se repiten, veamos cual nos comviene más, la letra T con la letra O nos da F y la letra X con O nos da J, ahora ambas nos dan como rsultados letras que tiene un frecuencia muy baja por lo que tomamos a la letra que le sigue que es la H que con O nos da T que tiene una mayor Frecuancia que las otras dos, por lo que la siguiente letra es la H que nos da T

Ahora veamos la lista 4

Lista 4
A = 35
B = 17
C = 15
D = 3
E = 0
F = 0
G = 4
H = 3
I = 56
J = 7
K = 8
L = 24
M = 44
N = 3
O = 2
P = 7
Q = 26
R = 1
S = 0
T = 22
U = 16
V = 23
W = 33
X = 6
Y = 4
Z = 30

Como podemos ver la lestras que mas se repiten son I y M que con la letra S nos dan Q y U, sin embargo nos percatamos que la letra que le sigue a esas es la letra A que con S nos da I que tiene un amyor Frecuencia que las otras dos por lo que tomamos a A que nos da I.

Finalmente veamos la lista 5.

Lista 5
A = 25
B = 37
C = 14
D = 2
E = 25
F = 27
G = 14
H = 11
I = 4
J = 0
K = 0
L = 4
M = 3
N = 48
O = 6
P = 15
Q = 24
R = 55
S = 6
T = 4
U = 4
V = 32
W = 0
X = 0
Y = 17
Z = 12

Como podemos ver las letras que más se repiten son R y M que con N nos dan E y A pero nos percatamos que utilizando las letras anteriores y alguna de estas dos el cifrado no nos daba algo choerente por lo que usamos la letra que le sigue que es la B pero sucedio lo mismo, por lo uqe utilizamos la que le sigue que es la A que nos dio la letra N y en efecto nos dio algp coherente, por lo que la ultima letra es la A que nos da N.

Quedandonos al final que la clave es la plabra "LATIN", que aplicandola al texto para decifrar nos da el siguiente texto

E N E SEL U G A R L A S E N O R A E L O D I A R E A L I Z AEL M I L A G R O A G
A R R A L O S P O C O S P E L O S R OJO S D E M I T I A Q U E Y A E S T A M E D
I O C A L V A DES P U E S L O S L A V A L O S S E C A L O S E S T I R A LES H A
C E C R E P E L O S E X T I E N D E Y L O S S O B AHA S T A T R A N S F O R M
A R L A E S C A S A C A B E L LER A D E M I T I A E N U N E D I F I C I O D E F A

N T A SIA D E V A R I O S P I S O S C O N R U L O S R I S O S C AIR E L E S Y R O
S E T O N E S L O H O R N E A D U R A N TEA L G U N A S H O R A S E N E L S E
C A D O R Y D E S P UES L O R O C I A C O N S I E T E L I T R O S D E L A C A
PAR A D A R L E F I R M E Z A Y S O S T E N A S U C R E A CIO N E L D I A D E L
A B O D A M I T I A L L E G O A N U EST R A C A S A C O N U N P E I N A D O Q
U E M E D I A D OSM E T R O S D E A L T U R A S E V E I A I M P R E S I O NAN
T E C U A N D O A B R I M O S L A P U E R T A P A R A SAL I R S E E S C U C H O
U N Z U M B I D O A L L E V A N TAR L A V I S T A A L C I E L O D E S C U B R I
M O S U N BIC H O Q U E S E A C E R C A B A V O L A N D O A T O D A VEL O C I
D A D Q U E E S E S O P R E G U N T O M I M A M AYO S E L O Q U E E S A C L A
R E T R I U N F A L C U A N DOL O P U D E D I S T I N G U I R M A S D E C E R C
A E S UNM A Y A T E Y E S O Q U E E S I N T E R R O G O M I H E RMA N A U N
M A Y A T E L E S I N F O R M E E S U N A E S PEC I E D E E S C A R A B A J O P
E R O U N P O C O M A S REC H O N C H O E L M A Y A T E E R A D E L M I S M
O C O LOR R O J O B R I L L A N T E Q U E E L C A B E L L O D E MIT I A E L I N
S E C T O V O L O E N P I C A D A Y Z A O SEZ A M B U L L O E N E L P E I N A D
O A Y Q U E A S C O GRI T O M I M A M A A Y Q U E S U S T O B E R R E O M I H
ERM A N A A Y Q U E B A R B A R I D A D S E H I S T E R I ZOM I T I A Q U I T E
N M E L O P E R O S I N D E S C O M PON E R E L P E I N A D O A D V I R T I O N
O S A S O M A MOS T E M E R O S O S A L A S P R O F U N D I D A D E S D EES A
S E L V A R O J A Y A L O V I D I J O M I P A P A E STA U N P O C O A T U R D I
D O Y M A R E A D O P O R E L OLO R D E L A L A C A S A L D E A H I E L M A Y
A T E N O OBE D E C I O L E M E T I M O S U N L A P I Z H U R G A M OSC O N E
L D E D O L E S O P L A M O S Y N A D A E L P E INA D O S E G U I A I N T A C T
O A D E N T R O D E N A D AVA L I E R O N S U P L I C A S A M E N A Z A S N I L
O S MAS R U D O S P R O C E D I M I E N T O S N I M O D O S E IMP A C I E N T
O M I P A P A S E N O S H A C E T A R D E TEN D R A S Q U E I R C O N E S O M
I T I A A U N Q U E N ERV I O S A S A B I A Q U E N O T E N I A O T R A A L T E
RNA T I V A L A F I E S T A T R A N S C U R R I A N O R M ALM E N T E P E R O
M I T I A S E S O B R E S A L T A B A ACA D A R A T O C U A N D O T E R M I N
A M O S D E C E N ARY E M P E Z O L A M U S I C A M I T I A A H O G O U N G
RIT O Q U E T E P A S A L E P R E G U N T E C R E O Q U E ELE S C A R A B A
J O E S T A B A I L A N D O S U S U R R OME A S O M E A L P E I N A D O Y E F
E C T I V A M E N T EEL E S C A R A B A J O R O J O E S T A B A B A I L A N D
OEL P R I M E R V A L S D E L A N O C H E O B S E R V E F ASC I N A D O Q U
E E L M E R E N G U E D E L P A S T E L DEB O D A S T E N I A G R A N D E S S
E M E J A N Z A S C ONE L P E I N A D O D E M I T I A L L E G O E L M O M E N
TOD E F E L I C I T A R A L O S N O V I O S M I T I A S E LEV A N T O C O M O T
O D O S Y A L A B R A Z A R A L A N OVI A Z Z E L E S C A R A B A J O D E C I D
I O V O L A R ENE L I N E R I O R D E L P E I N A D O Q U E E S E S E R UID O P
R E G U N T O L A N O V I A A L G O A S U S T A D APA R E C E Q U E V I E N E
D E T U C A B E Z A T I A E S MIA P A R A T O P A R A L A S O R D E R A R E S
P O N D I OEL L A C O N U N A S O N R I S A D E P A N I C O